Supplemento ordinario alla “Gazzetta Ufficiale” n. 143 del 20 giugno 2002 - Serie generale

Spediz. abb. post. 45% - art. 2, comma 20/b
Legge 23-12-1996, n. 662 - Filiale di Roma

PARTE PRIMA **Roma - Giovedì, 20 giugno 2002** SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DIREZIONE E REDAZIONE PRESSO IL MINISTERO DELLA GIUSTIZIA - UFFICIO PUBBLICAZIONE LEGGI E DECRETI - VIA ARENULA 70 - 00100 ROMA
AMMINISTRAZIONE PRESSO L’ISTITUTO POLIGRAFICO E ZECCA DELLO STATO - LIBRERIA DELLO STATO - PIAZZA G. VERDI 10 - 00100 ROMA - CENTRALINO 06 85081

N. 130

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 11 aprile 2002.

Norme di sicurezza per la tutela delle informazioni UE classificate di attuazione della Decisione del Consiglio dell’Unione europea del 19 marzo 2001.

SOMMARIO

DECRETI PRESIDENZIALI

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 11 maggio 2002.

Norme di sicurezza per la tutela delle informazioni UE classificate di attuazione della Decisione del Consiglio dell'Unione europea del 19 marzo 2001.

IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

Vista la legge 24 ottobre 1977, n. 801, recante «Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato», in particolare articoli 1, secondo comma, e 12;

Vista la Decisione 2001/264/CE del Consiglio, pubblicata nella Gazzetta Ufficiale delle Comunità europee n. L 101 dell'11 aprile 2001, in particolare l'articolo 2, paragrafo 2, che impone agli Stati membri di adottare le misure adeguate, in conformità alle disposizioni nazionali, per garantire che, nel trattamento di informazioni UE classificate all'interno dei rispettivi servizi ed edifici, siano rispettate le norme della medesima Decisione da parte di:

membri della Rappresentanza permanente d'Italia presso l'Unione europea, nonché membri di delegazioni nazionali che partecipano alle riunioni del Consiglio o dei suoi organi o che prendono parte ad altre attività del Consiglio;

altri membri della pubblica amministrazione, di soggetti privati e privati cittadini soggetti, in Italia o all'estero, alla giurisdizione dello Stato italiano;

contraenti esterni e personale distaccato dallo Stato presso il Segretariato generale del Consiglio dell'Unione europea che trattano informazioni UE classificate;

Visto il decreto del Presidente del Consiglio dei Ministri del 21 settembre 1999;

Viste le direttive del Presidente del Consiglio dei Ministri/Autorità nazionale per la sicurezza:

PCM-ANS 1/R - Norme unificate per la tutela del segreto di Stato - Volume I - Sistema di sicurezza - Edizione 1987 e successive modificazioni e integrazioni;

PCM-ANS 1/R - Norme unificate per la tutela del segreto di Stato - Volume II - Sicurezza delle comunicazioni ed organizzazioni e procedure del servizio cifra - Edizione 1994;

PCM-ANS 1/R - Norme unificate per la tutela del segreto di Stato - Volume III - Sicurezza industriale - Edizione 1993;

PCM-ANS 1/R - Norme unificate per la tutela del segreto di Stato - Volume I - Direttiva per la protezione delle informazioni coperte dal segreto di Stato trattate in sistemi di elaborazione automatica e/o elettronica dei dati (EAD) - Edizione 1993;

PCM-ANS COMSEC 256 (B) - Norme relative all'installazione di apparati elettrici elettronici che elaborano informazioni classificate - Edizione 1998;

Ritenuta l'esigenza di dare, per gli aspetti interni, piena attuazione alla predetta Decisione del Consiglio dell'Unione europea 2001/264/CE;

Consultato, ai sensi dell'art. 31, comma 2, della legge 31 dicembre 1996, n. 675, il Garante per la protezione dei dati personali;

ADOTTA

il seguente decreto:

Art. 1.

1. Per gli aspetti di rilevanza interna, piena e completa attuazione è data alla Decisione 2001/264/CE del Consiglio dell'Unione europea del 19 marzo 2001, che adotta le norme di sicurezza del Consiglio, pubblicata nella Gazzetta Ufficiale delle Comunità europee n. L 101 dell'11 aprile 2001, di cui all'allegato 1.

2. L'organizzazione nazionale per la sicurezza, istituita ai fini della tutela delle informazioni classificate, è di conseguenza aggiornata secondo le disposizioni contenute nell'allegato 2.

3. L'Autorità nazionale per la sicurezza prescrive le altre disposizioni di dettaglio per l'integrale attuazione delle norme di sicurezza contenute nella predetta Decisione, nell'ambito nazionale e nel rispetto della disciplina di protezione dei dati personali, eventualmente applicabile.

4. Il presente decreto è pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 11 aprile 2002

Il Presidente: BERLUSCONI

Registrato alla Corte dei conti il 13 maggio 2002
Ministeri istituzionali, rep. n. 1/R, foglio n. 20

ALLEGATO 1

DECISIONE DEL CONSIGLIO del 19 marzo 2001 che adotta le norme di sicurezza del Consiglio (2001/264/CE)

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 207, paragrafo 3,

vista la decisione 2000/396/CE, CECA, Euratom del Consiglio, del 5 giugno 2000, che adotta il regolamento interno del Consiglio [1], in particolare l'articolo 24,

considerando quanto segue:

(1) Per sviluppare le attività del Consiglio in settori che richiedono un certo grado di riservatezza occorre porre in essere un sistema di sicurezza globale riguardante il Consiglio, il Segretariato generale e gli Stati membri.

(2) Detto sistema dovrebbe combinare in un unico testo la materia disciplinata da tutte le precedenti decisioni e disposizioni nello stesso settore.

(3) In concreto, la maggior parte delle informazioni UE classificate CONFIDENTIEL UE (UE riservatissime) e oltre riguarderanno la politica comune in materia di sicurezza e di difesa.

(4) Per salvaguardare l'efficienza del sistema di sicurezza così posto in essere, gli Stati membri dovrebbero condividerne la responsabilità del funzionamento, adottando le necessarie misure a livello nazionale per il rispetto delle disposizioni della presente decisione nei casi in cui le loro autorità competenti e i loro funzionari trattino informazioni classificate UE.

(5) Il Consiglio accoglie favorevolmente l'iniziativa della Commissione di introdurre per la data di applicazione della presente decisione un sistema globale che sia in linea con gli allegati della stessa, allo scopo di assicurare il buon funzionamento del processo decisionale dell'Unione.

(6) Il Consiglio sottolinea l'importanza di associare, ove opportuno, il Parlamento europeo e la Commissione alle regole e alle norme di riservatezza necessarie per salvaguardare gli interessi dell'Unione e degli Stati membri.

(7) La presente decisione lascia impregiudicato l'articolo 255 del trattato e i relativi strumenti di attuazione.

(8) La presente decisione lascia impregiudicate le pratiche esistenti negli Stati membri per quanto riguarda l'informazione dei Parlamenti nazionali sulle attività dell'Unione,

DECIDE:

Articolo 1

Sono approvate le norme di sicurezza del Consiglio contenute nell'allegato.

Articolo 2

1. Il Segretario generale/Alto rappresentante adotta le misure adeguate per garantire che, nel trattare informazioni classificate UE, i funzionari e gli altri agenti del Segretariato generale del Consiglio (in seguito denominato: "SGC"), i contraenti esterni dell'SGC e il personale distaccato presso l'SGC nonché negli edifici del Consiglio e negli organismi UE decentrati rispettino le norme di cui all'articolo 1 [2].

---

[1] GU L 149 del 23.6.2000, pag. 21.
[2] Cfr. conclusioni del Consiglio del 10 novembre 2000.

2. Gli Stati membri adottano le misure adeguate, in conformità di accordi nazionali, per garantire che, nel trattamento di informazioni classificate UE, all'interno dei servizi e degli edifici siano rispettate le norme di cui all'articolo 1 da parte di:

a) membri delle Rappresentanze permanenti degli Stati membri presso l'Unione europea, nonché membri di delegazioni nazionali che partecipano alle riunioni del Consiglio o dei suoi organi o che prendono parte ad altre attività del Consiglio;

b) altri membri delle amministrazioni nazionali degli Stati membri che trattano informazioni classificate UE, che prestino servizio nel territorio degli Stati membri o all'estero; e

c) contraenti esterni e personale distaccato degli Stati membri che trattano informazioni classificate UE.

Gli Stati membri informano l'SGC delle misure adottate.

3. Le misure di cui ai paragrafi 1 e 2 sono adottate entro il 30 novembre 2001.

Articolo 3

Conformemente ai principi fondamentali e alle norme minime di sicurezza contenuti nella parte I dell'allegato, il Segretario generale/Alto rappresentante può adottare misure ai sensi della parte II, sezione I, punti 1 e 2, dell'allegato.

Articolo 4

A decorrere dalla data della sua applicazione, la presente decisione sostituisce:

a) la decisione 98/319/CE del Consiglio, del 27 aprile 1998, relativa alle modalità secondo cui i funzionari e gli agenti del Segretariato generale del Consiglio possono essere autorizzati ad accedere a informazioni classificate in possesso del Consiglio [(1)];

b) la decisione del Segretario generale/Alto rappresentante, del 27 luglio 2000, relativa alle misure di protezione delle informazioni classificate applicabili al Segretariato generale del Consiglio [(2)];

c) la decisione 433/97 del Segretario generale del Consiglio, del 22 maggio 1997, relativa alla procedura di nulla osta di sicurezza dei funzionari responsabili per il funzionamento della rete Cortesy.

Articolo 5

1. La presente decisione ha effetto il giorno della pubblicazione.

2. Essa si applica a decorrere dal 1 dicembre 2001.

Fatto a Bruxelles, addì 19 marzo 2001.

Per il Consiglio
Il Presidente
A. LINDH

(1) GU L 140 del 12.5.1998, pag. 12.
(2) GU C 239 del 23.8.2000, pag. 1.

ALLEGATO

NORME DI SICUREZZA DEL CONSIGLIO DELL'UNIONE EUROPEA

SOMMARIO

Appendici

PARTE I

PRINCIPI FONDAMENTALI E NORME MINIME DI SICUREZZA

INTRODUZIONE

1. Con queste disposizioni si stabiliscono i principi fondamentali e le norme minime di sicurezza che il Consiglio, il Segretariato generale del Consiglio (in seguito denominato "SGC"), gli Stati membri e gli organismi decentrati dell'Unione europea (in seguito denominati "organismi decentrati UE") devono debitamente rispettare perché sia salvaguardata la sicurezza e tutti abbiano la garanzia che è in vigore uno standard comune di protezione.

2. Con "informazioni classificate UE" si intendono le informazioni e i materiali la cui divulgazione non autorizzata potrebbe recare in varia misura pregiudizio agli interessi dell'UE o a uno o più Stati membri, sia che le informazioni suddette provengano dall'interno dell'UE ovvero dagli Stati membri, da Stati terzi o da organizzazioni internazionali.

3. Ai fini delle presenti norme si intende per:
   a) "documento", qualsiasi lettera, nota, verbale, relazione, promemoria, segnale/messaggio, schizzo, fotografia, diapositiva, pellicola, mappa, diagramma, piano, notebook, stencil, carta carbone, nastro dattilografico o per stampante, nastro, cassetta, dischetto di computer, CD ROM o altro mezzo materiale sul quale possono essere state registrate informazioni;
   b) "materiale", qualsiasi "documento" secondo la definizione di cui alla lettera a) e altresì qualsiasi elemento di equipaggiamento o di armi, sia sotto forma di prodotto finito sia in corso di lavorazione.

4. La sicurezza ha i seguenti obiettivi principali:
   a) a) proteggere le informazioni classificate UE dallo spionaggio, dalla violazione o dalla diffusione non autorizzata;
   b) b) salvaguardare le informazioni UE impiegate in sistemi e reti di comunicazione e informazioni da minacce contro la loro integrità e disponibilità;
   c) c) salvaguardare le installazioni in cui sono collocate le informazioni UE dal sabotaggio e dal danno intenzionale premeditato;
   d) d) nel caso fosse impossibile evitarlo, valutare il danno prodotto, limitarne le conseguenze ed adottare le misure necessarie per ripararlo.

5. Un'efficace sicurezza si fonda sui seguenti elementi:
   a) all'interno di ciascuno Stato membro un'organizzazione della sicurezza nazionale responsabile per:
      i) la raccolta e la registrazione di intelligence in materia di spionaggio, sabotaggio, terrorismo e altre attività sovversive;
      ii) l'informazione e la consulenza del proprio governo, e attraverso questo, del Consiglio, circa il carattere delle minacce che incombono sulla sicurezza e i relativi mezzi di protezione;
   b) all'interno di ciascuno Stato membro e nell'ambito dell'SGC, un'autorità tecnica INFOSEC responsabile per la cooperazione con l'autorità di sicurezza interessata, che ha lo scopo di fornire informazioni e consulenza circa le minacce tecniche che incombono sulla sicurezza e i relativi mezzi di protezione;
   c) una regolare collaborazione tra amministrazioni pubbliche, organismi e organi interessati dell'SGC per stabilire e raccomandare opportunamente:
      i) quali informazioni, risorse e installazioni occorre proteggere;
      ii) norme comuni di protezione.

6. Per quanto riguarda la riservatezza, la selezione delle informazioni e dei materiali da proteggere e la valutazione del grado di protezione necessaria richiedono diligenza ed esperienza. E' particolarmente importante che il grado di protezione corrisponda al grado di sicurezza richiesto dalla singola informazione e dal singolo materiale da proteggere. Perché non vi siano ostacoli al flusso delle informazioni occorre prendere provvedimenti per evitare la sovraclassificazione. Il sistema di classificazione è lo strumento per tradurre in pratica questi principi; un sistema di classificazione analogo dovrebbe essere adottato nella pianificazione e nell'organizzazione delle modalità per combattere lo spionaggio, il sabotaggio, il terrorismo e altre minacce in modo che godano della massima protezione i principali edifici in cui sono collocate informazioni classificate e i punti più sensibili all'interno di questi.

PRINCIPI BASILARI

7. Le misure di sicurezza:
   a) riguardano tutte le persone che hanno accesso alle informazioni classificate, ai supporti delle informazioni classificate, agli edifici che contengono tali informazioni e a importanti installazioni;
   b) sono destinate a individuare le persone la cui posizione possa mettere a repentaglio la sicurezza di informazioni classificate e di importanti installazioni che contengono informazioni classificate e a provvedere alla loro esclusione o allontanamento;
   c) impediscono alle persone non autorizzate di accedere alle informazioni classificate o alle installazioni che le contengono;
   d) garantiscono che le informazioni classificate siano diffuse soltanto in base al principio della necessità di sapere che è fondamentale per tutti gli aspetti della sicurezza;
   e) assicurano l'integrità (ossia la prevenzione della corruzione, dell'alterazione o della cancellazione non autorizzata) e la disponibilità (ossia l'accesso non è negato a coloro che devono e sono autorizzati ad averlo) di tutte le informazioni, siano esse classificate o non, e soprattutto delle informazioni immagazzinate, elaborate o trasmesse sotto forma elettromagnetica.

ORGANIZZAZIONE DELLA SICUREZZA

Norme comuni minime

8. Il Consiglio e ciascuno Stato membro garantiscono che nelle amministrazioni locali e/o governative, presso altre istituzioni, altri organismi e contraenti UE siano osservate norme minime comuni di sicurezza in modo che informazioni classificate UE possano essere fornite confidando che siano trattate con la stessa diligenza. Dette norme minime includono criteri per il nulla osta di sicurezza del personale e procedure per la protezione delle informazioni classificate UE.

SICUREZZA DEL PERSONALE

Nulla osta di sicurezza del personale

9. Tutti coloro che devono accedere a informazioni classificate CONFIDENTIEL UE (UE riservatissime) o oltre devono aver debitamente ricevuto il nulla osta prima di essere autorizzate a tale accesso. Lo stesso nulla osta è richiesto alle persone che si occupano del funzionamento tecnico o della manutenzione dei sistemi di comunicazione e di informazione contenenti informazioni classificate. Questo nulla osta deve servire a determinare se detti individui:

   a) a) sono di indefettibile lealtà;
   b) b) dimostrano forza di carattere e discrezione tali che non vi siano dubbi sulla loro integrità nel trattamento delle informazioni classificate ovvero;
   c) c) possono essere sensibili a pressioni provenienti dall'esterno o altre, per esempio a causa di soggiorni precedenti o frequentazioni passate che possono costituire un rischio per la sicurezza.

   A un esame particolarmente accurato nell'ambito delle procedure di nulla osta sono sottoposti coloro che:

   d) d) devono ottenere accesso alle informazioni TRES SECRET UE/EU TOP SECRET (UE segretissimo);
   e) e) occupano posizioni per le quali hanno normale accesso a una considerevole quantità di informazioni SECRET EU (UE segreto);
   f) f) hanno per le loro mansioni accesso speciale a sistemi di comunicazione o di informazioni essenziali per le missioni e perciò possono avere accesso non autorizzato a grandi quantità di informazioni classificate UE o danneggiare gravemente la missione con atti di sabotaggio tecnico.

   Nelle circostanze di cui alle lettere d), e) e f) deve farsi il massimo uso possibile della tecnica delle indagini di fondo.

10. Le persone che non hanno una vera e propria necessità di sapere e lavorano in circostanze nelle quali possono avere accesso a informazioni classificate UE (per esempio fattorini, agenti della sicurezza, personale addetto alla manutenzione o alle pulizie ecc.), devono prima di tutto ottenere un debito nulla osta di sicurezza.

Registrazione dei nulla osta del personale

11. Tutti i servizi, organi o installazioni che trattano informazioni classificate UE ovvero ospitano sistemi di comunicazione o di informazioni essenziali per le missioni tengono una traccia dei nulla osta concessi al personale addetto. Ciascun nulla osta deve essere verificato secondo le esigenze, affinché si abbia la garanzia che è adatto ai compiti svolti da quella persona; deve essere immediatamente riesaminato non appena nuove informazioni indichino che non è più nell'interesse della sicurezza mantenere quella persona a contatto con le informazioni classificate. E' il capo della sicurezza per il servizio, organismo o installazione interessata a custodire la traccia dei nulla osta.

Istruzioni di sicurezza per il personale

12. Tutto il personale che ricopre incarichi in cui potrebbe aver accesso a informazioni classificate è dettagliatamente istruito al momento di assumere l'incarico e a intervalli regolari circa la necessità della sicurezza e le relative procedure. Occorre esigere che tutto il personale di cui trattasi certifichi per iscritto di aver perfettamente compreso le norme di sicurezza connesse alle sue mansioni.

Responsabilità dei dirigenti

13. I dirigenti hanno il dovere di sapere quali dei loro subordinati lavorino a contatto di informazioni classificate o abbiano accesso a sistemi di comunicazione o di informazioni sensibili per le missioni e di registrare e riferire circa qualsiasi incidente o caso di palese vulnerabilità che possa avere conseguenze sulla sicurezza.

Status del personale in fatto di sicurezza

14. Sono poste in essere procedure per garantire che, allorché si viene a conoscenza di informazioni negative riguardo all'individuo, si chiarisca se costui svolge un lavoro connesso con le informazioni classificate ovvero ha accesso a sistemi di comunicazione o di informazioni essenziali per le missioni e se le autorità interessate ne siano informate. Se si stabilisce che rappresenta un pericolo per la sicurezza, detto individuo deve essere allontanato o rimosso dal suo incarico nel quale potrebbe mettere a repentaglio la sicurezza.

SICUREZZA MATERIALE

Necessità della protezione

15. Il grado di sicurezza materiale da applicare per garantire la protezione delle informazioni classificate UE deve essere proporzionato alla classificazione, al volume e alle minacce che incombono sulle informazioni e sul materiale custodito. Occorrerà perciò evitare sia la sovraclassificazione sia la sottoclassificazione e la classificazione deve essere oggetto di regolare revisione. Tutti i detentori di informazioni classificate UE devono seguire pratiche uniformi per quanto riguarda la classificazione delle informazioni in loro possesso e ottemperare a norme comuni di protezione per quel che riguarda la custodia, la trasmissione e la diffusione di informazioni e di materiale soggetti a protezione.

Controlli

16. Prima di lasciare i luoghi in cui sono riposte informazioni classificate UE non sottoposti a sorveglianza le persone a cui detti luoghi sono affidati devono assicurarsi che le informazioni siano immagazzinate in modo sicuro e che tutti i dispositivi di sicurezza siano stati attivati (serrature, allarmi, ecc.). Al termine dell'orario di lavoro devono essere effettuati altri controlli indipendenti.

Sicurezza degli edifici

17. Gli edifici contenenti informazioni classificate UE o sistemi di comunicazione e informazioni essenziali per le missioni devono essere protetti contro l'accesso non autorizzato. Il tipo di protezione destinato alle informazioni classificate UE, per esempio sbarramento di finestre, serrature alle porte, guardie all'entrata, sistemi di controllo dell'accesso automatizzati, controlli di sicurezza e ispezioni, sistemi d'allarme, sistemi di individuazione delle intrusioni e cani da guardia dipendono:

a) a) dalla classificazione, dal volume e dall'ubicazione all'interno dell'edificio delle informazioni e dei materiali da proteggere;

b) b) dalla qualità dei contenitori di sicurezza per queste informazioni e materiali;

c) c) dalle caratteristiche dell'edificio e dalla sua ubicazione.

18. Anche nel caso dei sistemi di comunicazione e di informazioni il tipo di protezione prescelto deve dipendere da una stima del valore di quanto è in gioco e del danno potenziale che deriverebbe dal venir meno della sicurezza, dalle caratteristiche e dall'ubicazione dell'edificio nel quale è custodito il sistema e dalla collocazione del sistema all'interno dell'edificio.

Piani d'emergenza

19. Occorre predisporre in anticipo piani dettagliati per la protezione delle informazioni classificate durante un'emergenza locale o nazionale.

SICUREZZA DELLE INFORMAZIONI (INFOSEC)

20. L'Infosec riguarda l'individuazione e l'applicazione di misure di sicurezza per proteggere le informazioni elaborate, immagazzinate o trasmesse in sistemi elettronici di comunicazione e di informazioni ed altri contro il venir meno della riservatezza, dell'integrità o della disponibilità, accidentale o intenzionale. Adeguate contromisure devono essere prese per prevenire l'accesso alle informazioni UE da parte di utenti non autorizzati, per impedire che a utenti autorizzati sia opposto il rifiuto di accedere alle informazioni UE e per prevenire l'alterazione ovvero la modificazione o la cancellazione non autorizzata di informazioni UE.

MISURE CONTRO IL SABOTAGGIO ED ALTRE FORME DI DANNO INTENZIONALE PREMEDITATO

21. Le precauzioni materiali per la protezione di importanti installazioni in cui sono conservate informazioni classificate sono la migliore garanzia di sicurezza e di protezione contro il sabotaggio e il danno intenzionale premeditato, laddove il solo nulla osta del personale non basta. L'organismo nazionale competente deve raccogliere intelligence circa lo spionaggio, il sabotaggio e il terrorismo ed altre attività sovversive.

COMUNICAZIONE DI INFORMAZIONI CLASSIFICATE A STATI TERZI O ORGANIZZAZIONI INTERNAZIONALI

22. E' compito del Consiglio decidere se comunicare a uno Stato terzo o a un'organizzazione internazionale informazioni classificate UE. Se l'originatore delle informazioni che si vogliono comunicare non è il Consiglio, questo deve anzitutto ottenere il consenso dell'originatore. Se è impossibile stabilire l'originatore, il Consiglio deve assumersi la responsabilità.

23. Le informazioni classificate che il Consiglio riceve da Stati terzi, da organizzazioni internazionali o da altri terzi devono essere oggetto di protezione proporzionata alla loro classificazione ed equivalente alle norme qui stabilite per informazioni classificate UE o alle norme più severe richieste dai terzi che comunicano l'informazione. Possono essere predisposti controlli reciproci.

24. I principi di cui sopra devono essere applicati in conformità delle disposizioni dettagliate della parte II.

PARTE II

SEZIONE I

ORGANIZZAZIONE DELLA SICUREZZA NEL CONSIGLIO DELL'UNIONE EUROPEA

Il Segretario generale/Alto rappresentante

1. Il Segretario generale/Alto rappresentante

   a) attua la politica di sicurezza del Consiglio;

   b) prende in esame i problemi di sicurezza sottopostigli dal Consiglio o dagli organi competenti di questo;

   c) esamina le questioni che comportano cambiamenti nella politica di sicurezza del Consiglio in stretto legame con le autorità di sicurezza nazionali (o altre) degli Stati membri (in seguito denominate "NSA"). Un elenco di dette autorità è contenuto nell'appendice I.

2. In particolare il Segretario generale/Alto rappresentante è responsabile per

   a) il coordinamento di tutte le questioni di sicurezza connesse alle attività del Consiglio;

   b) esigere dagli Stati membri di predisporre un registro centrale TRES SECRET UE/EU TOP SECRET (UE segretissimo) e chiedere che siffatto registro sia predisposto eventualmente negli organismi decentrati UE;

   c) inviare alle autorità designate dagli Stati membri le richieste affinché gli NSA predispongano i nulla osta di sicurezza per il personale impiegato nell'SGC in conformità della sezione VI;

   d) fare ordinare indagini riguardo a qualsiasi fuga di notizie circa informazioni classificate UE, che a prima vista sembri avere avuto luogo nell'SGC o in uno degli organismi decentrati UE;

   e) chiedere alle autorità di sicurezza interessate di avviare indagini nel caso di fughe di notizie circa informazioni classificate UE che sembrino aver avuto luogo al di fuori dell'SGC o di un organismo decentrato UE e coordinare le inchieste quando sono coinvolte più autorità di sicurezza;

   f) compiere insieme e d'accordo con l'NSA interessata esami periodici della normativa sulla sicurezza per la protezione delle informazioni classificate UE negli Stati membri;

   g) mantenere uno stretto legame con tutte le autorità per la sicurezza interessate ai fini di un coordinamento globale della sicurezza;

   h) riesaminare costantemente la politica e le procedure di sicurezza del Consiglio e se necessario predisporre le opportune raccomandazioni. Al riguardo egli presenta al Consiglio il piano di ispezione annuale predisposto dal Servizio di sicurezza dell'SGC.

Comitato per la sicurezza del Consiglio

3. E' istituito un Comitato per la sicurezza. Ne fanno parte rappresentanti delle NSA degli Stati membri. E' presieduto dal Segretario generale/Alto rappresentante o dal suo delegato. Possono essere invitati a parteciparvi rappresentanti degli organismi decentrati UE quando vi si discutono questioni che li riguardano.

4. Il Comitato di sicurezza si riunisce secondo le istruzioni del Consiglio, a richiesta del Segretario generale/Alto rappresentante o di una NSA. Il Comitato ha facoltà di esaminare e valutare tutti i problemi di sicurezza relativi ai lavori del Consiglio e di presentare opportune raccomandazioni a quest'ultimo. Per quanto riguarda l'attività dell'SGC il Comitato ha il potere di fare raccomandazioni su problemi di sicurezza al Segretario generale/Alto rappresentante.

Servizio di sicurezza del Segretariato generale del Consiglio

5. Per adempiere le responsabilità di cui ai paragrafi 1 e 2 il Segretario generale/Alto rappresentante dispone del Servizio di sicurezza dell'SGC per il coordinamento, la supervisione e l'applicazione delle misure di sicurezza.

6. Il capo del Servizio di sicurezza dell'SGC è il consigliere principale del Segretario generale/Alto rappresentante circa le questioni di sicurezza e funge da segretario del Comitato per la sicurezza. Al riguardo dirige l'aggiornamento della normativa in merito alla sicurezza e coordina le misure di sicurezza con le autorità competenti degli Stati membri e, se opportuno, con le organizzazioni internazionali collegate al Consiglio mediante accordi in materia di sicurezza. Allo scopo agisce come ufficiale di collegamento.

7. Il capo del Servizio di sicurezza dell'SGC è responsabile dell'accreditamento dei sistemi e delle reti di TI all'interno dell'SGC. Il capo del Servizio di sicurezza dell'SGC e la relativa NSA decidono insieme, se opportuno, circa l'accreditamento dei sistemi e delle reti di TI che coinvolgono l'SGC, gli Stati membri e gli organismi decentrati UE o i terzi (Stati o organizzazioni internazionali).

Organismi decentrati UE

8. I direttori degli organismi decentrati UE sono responsabili dell'attuazione della sicurezza all'interno dell'edificio. Di norma affidano la responsabilità a un membro del personale, che è designato come funzionario responsabile della sicurezza.

Stati membri

9. Ciascuno Stato membro designa un responsabile NSA per la sicurezza delle informazioni classificate UE [1].

10. Nel quadro di ciascuna amministrazione nazionale la relativa NSA è responsabile per:

   a) Il mantenimento della sicurezza delle informazioni classificate UE custodite da un dipartimento, un organo o organismo nazionale, sia esso pubblico o privato, nel paese o all'estero;

   b) autorizzare la costituzione di registri TRES SECRET UE/EU TOP SECRET (UE segretissimo) (questa facoltà può essere delegata all'ufficiale di controllo TRES SECRET UE/EU TOP SECRET (UE segretissimo) di un ufficio centrale di registrazione;

   c) l'ispezione periodica dei dispositivi di sicurezza per la protezione delle informazioni classificate UE;

   d) garantire che tutti i cittadini e gli stranieri impiegati in un dipartimento, organo o organismo nazionale che possano avere accesso a informazioni classificate TRES SECRET UE/EU TOP SECRET (UE segretissime), SECRET UE (UE segrete) e CONFIDENTIEL UE (UE riservatissime) abbiano ottenuto il nulla osta di sicurezza;

   e) concepire i piani di sicurezza necessari per impedire che le informazioni classificate UE finiscano in mano a persone non autorizzate.

Ispezioni reciproche di sicurezza

11. Il Servizio di sicurezza dell'SGC e le NSA interessate, insieme e d'accordo tra loro, compiono ispezioni periodiche dei dispositivi di sicurezza per la protezione delle informazioni classificate UE nell'SGC e nelle Rappresentanze permanenti degli Stati membri presso l'Unione europea oltreché negli uffici degli Stati membri negli edifici del Consiglio [2].

12. Il Servizio di sicurezza dell'SGC ovvero, a richiesta del Segretariato generale, la NSA dello Stato membro ospitante, compiono ispezioni periodiche della normativa di sicurezza per la protezione delle informazioni classificate UE negli organismi decentrate UE.

[1] Un elenco delle responsabili della sicurezza delle informazioni classificate UE è contenuto nell'appendice 1.
[2] Fatta salva la convenzione di Vienna del 1961 sulle relazioni diplomatiche.

SEZIONE II

CLASSIFICAZIONI E CONTRASSEGNI

LIVELLI DI CLASSIFICAZIONE [1]

Le informazioni sono classificate ai seguenti livelli:

1. TRÈS SECRET UE/EU TOP SECRET: questa classificazione si applica soltanto a informazioni e materiali la cui divulgazione non autorizzata potrebbe arrecare danni di eccezionale gravità agli interessi fondamentali dell'Unione europea o di uno o più Stati membri.

2. SECRET UE: questa classificazione si applica soltanto a informazioni e materiali la cui divulgazione non autorizzata potrebbe ledere gravemente gli interessi fondamentali dell'Unione europea o di uno o più Stati membri.

3. CONFIDENTIEL UE: questa classificazione si applica a informazioni e materiale la cui divulgazione non autorizzata potrebbe ledere gli interessi fondamentali dell'Unione europea o di uno o più Stati membri.

4. RESTREINT UE: questa classificazione si applica a informazioni e materiali la cui divulgazione non autorizzata potrebbe arrecare danno agli interessi dell'Unione europea o di uno o più Stati membri.

CONTRASSEGNI

5. Un contrassegno di limitazione può essere usato per specificare un settore che fa parte del documento o una distribuzione particolare sulla base del principio della necessità di sapere.

6. Il contrassegno ESDP/PESD si appone su documenti e copie degli stessi per quanto riguarda la sicurezza e la difesa dell'Unione o di uno o più Stati membri o riguardo alla gestione delle crisi militare o non militare.

7. Taluni documenti, in particolare quelli che si riferiscono ai sistemi di tecnologia dell'informazione (TI) possono recare un altro contrassegno che implica misure di sicurezza supplementari, come definito nella normativa appropriata.

APPOSIZIONE DELLE CLASSIFICAZIONI E CONTRASSEGNI

8. La classificazione e i contrassegni si applicano come segue:

   a) su documenti RESTREINT UE (UE riservato) con mezzi meccanici o elettronici,

   b) su documenti CONFIDENTIEL UE (UE riservatissimo) con mezzi meccanici e a mano o a stampa su carta prestampigliata, registrata,

   c) su documenti SECRET UE (UE segreto) e TRES SECRET UE/EU TOP SECRET (UE segretissimo) con mezzi meccanici e a mano.

---

[1] Nell'appendice 2 è contenuta una tabella comparativa delle classificazioni di sicurezza UE, NATO, UEO, e degli Stati membri.

SEZIONE III

GESTIONE DELLA CLASSIFICAZIONE

1. Le informazioni sono classificate solo ove necessario. La classificazione è indicata chiaramente e correttamente ed è mantenuta solo per la durata in cui è necessario proteggere l'informazione.

2. La responsabilità della classificazione dell'informazione e di eventuali declassamenti o declassificazioni [1] successivi spetta unicamente all'originatore.

   Il funzionario o altro agente dell'SGC classifica un'informazione, oppure la declassa o la declassifica su istruzione del suo direttore generale o d'intesa con il medesimo.

3. Le modalità dettagliate per il trattamento dei documenti classificati sono state elaborate in modo da garantire che essi siano soggetti a una protezione commisurata alle informazioni che contengono.

4. Il numero di persone autorizzate ad emanare documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) è limitato al minimo e il loro nominativo figura in un elenco elaborato dall'SGC, da ogni Stato membro e, se opportuno, da ogni organismo decentrato dell'UE.

ATTRIBUZIONE DELLE CLASSIFICAZIONI

5. La classificazione di un documento è determinata dal livello di sensibilità del suo contenuto, ai sensi della definizione di cui alla sezione II, punti da 1 a 4. E' importante che la classificazione sia attribuita correttamente e con moderazione, in particolare per quanto riguarda la classificazione TRES SECRET UE/EU TOP SECRET (UE segretissimo).

6. L'originatore di un documento che deve essere classificato tiene presente le disposizioni sopraelencate e limita la tendenza alla sovra o sottoclassificazione.

   Anche se un grado di classificazione elevato sembra garantire a prima vista una maggiore protezione del documento, la sovraclassificazione abituale può condurre ad una perdita di fiducia nella validità del sistema di classificazione.

   D'altro canto, i documenti non devono essere sottoclassificati nella prospettiva di aggirare i vincoli connessi con la protezione.

   Nell'appendice 3 figura una guida pratica per la classificazione.

7. E' possibile che singole pagine, paragrafi, sezioni, annessi, appendici, allegati di un determinato documento e altro materiale accluso richiedano classificazioni differenti: in tal caso essi sono contraddistinti di conseguenza e a tutto il documento viene attribuito il grado di classificazione dell'elemento con grado di classificazione più elevato.

8. Il grado di classificazione attribuito a una lettera o nota cui è accluso altro materiale corrisponde a quello dell'elemento accluso con grado più elevato. L'originatore indica chiaramente il grado di classificazione da attribuire alla lettera o nota quando è separata dal materiale accluso.

DECLASSAMENTO E DECLASSIFICAZIONE

9. I documenti classificati UE possono essere declassati o declassificati unicamente con il consenso dell'originatore e, se necessario, previa discussione con le altre parti interessate. Il declassamento o la declassificazione sono confermati per iscritto. L'istituzione, lo Stato membro, l'ufficio, l'organizzazione successiva o l'alta autorità da cui ha origine il documento sono tenuti ad informare i destinatari del cambiamento di classificazione e questi ultimi sono a loro volta tenuti ad informarne i destinatari successivi ai quali hanno trasmesso l'originale o una copia del documento.

10. Nella misura del possibile, l'originatore indica sul documento classificato la data o un termine a partire dal quale le informazioni in esso contenute potranno essere declassate o declassificate. In caso contrario, esso verifica almeno ogni cinque anni che la classificazione iniziale del documento sia tuttora necessaria.

---

[1] Per declassamento («downgrading») si intende una riduzione del grado di classificazione. Per declassificare («declassification») si intende la soppressione di qualsiasi menzione di classificazione.

SEZIONE IV

SICUREZZA MATERIALE

DISPOSIZIONI GENERALI

1. Scopo principale delle misure di sicurezza materiale è evitare che le persone non autorizzate abbiano accesso alle informazioni e/o al materiale classificato UE.

REQUISITI DI SICUREZZA

2. Tutti i locali, zone, edifici, uffici, stanze, sistemi di comunicazione e d'informazione, ecc. in cui sono custoditi e/o trattati informazioni e materiale classificato UE sono protetti da adeguate misure di sicurezza materiale.

3. Per la decisione sul grado di protezione materiale necessario occorre tener conto di tutti i fattori pertinenti, quali:

   a) il grado di classificazione dell'informazione e/o del materiale;

   b) la quantità e la forma (ad esempio supporto cartaceo, mezzi di archiviazione elettronica) delle informazioni detenute;

   c) la minaccia in loco rappresentata da servizi segreti che prendono di mira l'UE, gli Stati membri e/o altre istituzioni o terzi in possesso di informazioni classificate UE, nonché segnatamente da atti di sabotaggio, terrorismo e altri atti sovversivi e/o criminali.

4. Le misure di sicurezza materiale applicate sono volte a:

   a) impedire agli intrusi l'ingresso fraudolento o con la forza;

   b) dissuadere, impedire e scoprire azioni da parte di personale in malafede (cosiddette "talpe");

   c) evitare che funzionari o altri agenti dell'SGC, di dipartimenti governativi degli Stati membri e/o di altre istituzioni nonché terzi che non hanno necessità di sapere possano accedere alle informazioni classificate UE.

MISURE DI SICUREZZA MATERIALE

Zone di sicurezza

5. Le zone in cui sono trattate e custodite le informazioni classificate CONFIDENTIEL UE (UE riservatissimo) o di grado superiore sono organizzate e strutturate in modo da corrispondere a uno dei seguenti parametri:

   a) zona di sicurezza di categoria I: zona in cui sono trattate e custodite informazioni CONFIDENTIEL UE (UE riservatissimo) o di grado superiore in modo che l'ingresso in tale zona rappresenti, a tutti i fini pratici, l'accesso alle informazioni classificate. Per tale zona occorre prevedere:

      i) un perimetro chiaramente delimitato e protetto attraverso cui controllare tutti gli ingressi e le uscite;

      ii) un sistema di controllo all'entrata che consenta l'ingresso solo alle persone in possesso di debito nulla osta di sicurezza e espressamente autorizzate ad entrare in tale zona;

      iii) la specificazione della classificazione attribuita all'informazione normalmente custodita nella zona in questione, ossia l'informazione cui si accede entrando in tale zona;

   b) zona di sicurezza di categoria II: zona in cui sono trattate e custodite informazioni CONFIDENTIEL UE (UE riservatissimo) o di grado superiore in modo da proteggerle da un accesso di persone non autorizzate mediante controlli interni, ad esempio locali in cui si trovano gli uffici in cui vengono di solito trattate e custodite le informazioni CONFIDENTIEL UE (UE riservatissimo) o di grado superiore. Per tale zona occorre prevedere:

      i) un perimetro chiaramente delimitato e protetto attraverso cui controllare tutti gli ingressi e le uscite;

      ii) un sistema di controllo all'entrata che consenta l'ingresso senza scorta solo alle persone in possesso di debito nulla osta di sicurezza ed espressamente autorizzate ad entrare in tale zona. Per tutte le altre persone occorre prevedere scorte o controlli equivalenti per evitare l'accesso non autorizzato alle informazioni classificate UE e l'ingresso non controllato a zone soggette a ispezioni tecniche di sicurezza.

Le zone non occupate da personale in servizio 24 ore al giorno sono ispezionate immediatamente dopo il normale orario di lavoro per garantire che le informazioni classificate UE siano correttamente protette.

Zona amministrativa

6. In prossimità delle zone di sicurezza di categoria I e II o per accedere a tali zone, può essere creata una zona amministrativa con minor livello di sicurezza. Occorre prevedere un perimetro chiaramente delimitato per l'ispezione del personale e dei veicoli. Nella zona amministrativa sono trattate e custodite solo informazioni classificate RESTREINT (UE riservato).

Controlli all'entrata e all'uscita

7. L'ingresso a zone di sicurezza delle categorie I e II è controllato da un lasciapassare o da un sistema di riconoscimento personale che si applica all'organico. E' altresì predisposto un sistema di controllo dei visitatori al fine di impedire l'accesso non autorizzato ad informazioni classificate UE. I sistemi di lasciapassare possono essere completati da altri di identificazione automatizzata, senza che ciò sostituisca totalmente il personale del servizio di sicurezza. Una modifica nella valutazione del rischio può comportare un rafforzamento delle misure di controllo delle entrate e delle uscite, per esempio durante la visita di personalità.

Ronde di controllo

8. Le ronde di controllo delle zone di sicurezza di categoria I e II vengono effettuate al di fuori del normale orario di lavoro per proteggere i beni dell'UE dal rischio di manomissioni, danni o perdite. Le ronde sono effettuate secondo una frequenza determinata dalle circostanze locali ma, come orientamento generale, ogni due ore.

Contenitori di sicurezza e camere blindate

9. Le informazioni classificate UE sono custodite in contenitori suddivisi in tre categorie:

   - Categoria A: contenitori approvati a livello nazionale per custodire informazioni classificate TRES SECRET UE/EU TOP SECRET (UE segretissimo) nelle zone di sicurezza delle categorie I e II;
   - Categoria B: contenitori approvati a livello nazionale per custodire informazioni classificate SECRET UE (UE segreto) e CONFIDENTIEL UE (UE riservatissimo) nelle zone di sicurezza delle categorie I e II;
   - Categoria C: mobili da ufficio atti a custodire solo le informazioni classificate RESTREINT UE (UE riservato).

10. Nelle camere blindate costruite in una zona di sicurezza della categoria I o II, e in tutte le zone di sicurezza della categoria I in cui sono custodite le informazioni classificate CONFIDENTIEL UE (UE riservatissimo) o di grado superiore in scaffali aperti o in cui si visualizzano prospetti, piantine, ecc., le pareti, il pavimento ed il soffitto, la o le porte provviste di serratura o serrature sono omologate da una NSA per garantire che offrano una protezione equivalente alla categoria di contenitore di sicurezza approvato per custodire informazioni con lo stesso grado di classificazione.

Dispositivi di chiusura

11. I dispositivi di chiusura utilizzati per i contenitori di sicurezza e le camere blindate in cui sono custodite informazioni classificate UE devono soddisfare i seguenti requisiti:

    - Gruppo A: approvati a livello nazionale per contenitori della categoria A;
    - Gruppo B: approvati a livello nazionale per contenitori della categoria B;
    - Gruppo C: idonei solo per i mobili da ufficio della categoria C.

Controllo delle chiavi e delle combinazioni

12. Le chiavi dei contenitori di sicurezza non possono essere asportate dall'edificio. La combinazione dei contenitori di sicurezza deve essere conosciuta a memoria dalle persone che ne fanno uso. Il capo della sicurezza dell'edificio in questione ha la responsabilità delle chiavi di riserva e di tutte le combinazioni, conservate in singoli plichi opachi sigillati, di cui far uso in caso di emergenza. Le chiavi, le chiavi di riserva e le combinazioni sono custodite in contenitori di sicurezza separati. Le chiavi e le combinazioni ricevono almeno la stessa protezione riservata al materiale cui danno accesso.

13. La combinazione dei contenitori di sicurezza è portata a conoscenza del minor numero di persone possibile. Le combinazioni vengono sostituite:

    a) al ricevimento di ogni nuovo contenitore;

    b) ad ogni cambiamento di personale;

    c) ad ogni manomissione effettiva o sospettata;

    d) ad intervalli possibilmente semestrali, e per lo meno ogni dodici mesi.

Dispositivi per il rilevamento di intrusi

14. Quando le informazioni classificate UE sono protette da sistemi di allarme, televisione a circuito chiuso e altri dispositivi elettrici, si prevede un'erogazione di elettricità di emergenza per garantire il funzionamento ininterrotto del sistema in caso di avaria del sistema centrale. E' altresì indispensabile che in caso di disfunzione o di manomissione di detti sistemi, venga attivato un allarme o un altro segnale affidabile per il servizio di sicurezza.

Attrezzatura approvata

15. Le NSA mantengono, da sole o con le NSA di un altro Paese, elenchi aggiornati suddivisi per tipo e modello dell'attrezzatura di sicurezza da essi approvata per la protezione diretta o indiretta delle informazioni classificate in base a varie circostanze e condizioni specificate. Il servizio di sicurezza dell'SGC mantiene un elenco analogo che si basa, tra l'altro, sulle informazioni fornite dalle NSA. Prima dell'acquisto di tali attrezzature gli organi decentrati dell'UE si consultano con il servizio di sicurezza dell'SGC e, se del caso, con la NSA dello Stato membro che le ospita.

Protezione materiale delle fotocopiatrici e dei fax

16. Le fotocopiatrici e i fax sono protetti materialmente per quanto necessario a garantire che solo le persone autorizzate possano usarli e che tutti i documenti classificati da essi prodotti siano soggetti a opportuni controlli.

PROTEZIONE CONTRO SGUARDI E ASCOLTI INDISCRETI

Sguardi indiscreti

17. Per garantire che le informazioni classificate UE non siano visionate, anche accidentalmente, da persone non autorizzate devono essere prese tutte le misure appropriate, sia di giorno che di notte.

Ascolti indiscreti

18. Gli uffici o le zone in cui si discutono regolarmente informazioni classificate SECRET UE (UE segreto) o di grado superiore sono protetti dall'ascolto indiscreto attivo e passivo qualora il rischio lo richieda. La valutazione del rischio del verificarsi di questo evento spetta alle autorità di sicurezza competenti, eventualmente previa consultazione delle NSA.

19. Per decidere le misure di protezione che occorre prendere nei locali che possono essere soggetti ad ascolto indiscreto passivo (per esempio, isolamento dei muri, delle porte, del pavimento e del soffitto, misurazione delle emissioni compromettenti) e all'ascolto indiscreto attivo (per esempio, ricerca di microfoni), il servizio di sicurezza dell'SGC può chiedere l'assistenza di esperti delle NSA. I capi della sicurezza degli organismi decentrati dell'UE possono chiedere al servizio di sicurezza dell'SGC di procedere ad ispezioni tecniche e/o possono richiedere l'assistenza di esperti delle NSA.

20. Parimenti, su richiesta del capo della sicurezza competente, quando le circostanze lo rendano necessario, specialisti della sicurezza tecnica presso le NSA possono ispezionare il materiale per le telecomunicazioni e qualsiasi tipo di attrezzatura elettrica o elettronica da ufficio utilizzata durante le riunioni di livello SECRET UE (UE segreto) e di grado superiore.

ZONE TECNICAMENTE SICURE

21. Alcune zone possono essere designate come zone tecnicamente sicure, per le quali è previsto un controllo speciale all'ingresso. Quando non vengono occupate tali zone sono chiuse a chiave mediante una procedura convenuta, e tutte le chiavi sono considerate chiavi di sicurezza. Queste zone sono soggette a regolari ispezioni materiali, cui si procederà anche dopo ogni ingresso non autorizzato, effettivo o sospettato.

22. Si procede ad un inventario particolareggiato dell'attrezzatura e dei mobili per controllarne la movimentazione. In queste zone non possono essere introdotti mobili o altra attrezzatura che non siano stati precedentemente verificati con cura dal personale di sicurezza avente una formazione specifica per rilevare qualsiasi meccanismo di ascolto. Come regola generale, nelle zone tecnicamente sicure occorre evitare l'installazione di linee per la comunicazione.

SEZIONE V

REGOLE GENERALI RELATIVE AL PRINCIPIO "NEED TO KNOW" (NECESSITÀ DI SAPERE) E AL NULLA OSTA DI SICUREZZA

1. L'accesso alle informazioni classificate UE è consentito solo alle persone che hanno necessità di sapere per lo svolgimento delle loro funzioni o missioni. L'accesso alle informazioni TRES SECRET UE/EU TOP SECRET (UE segretissimo), SECRET UE (UE segreto) e CONFIDENTIEL UE (UE riservatissimo) è autorizzato solo per le persone in possesso dell'appropriato nulla osta di sicurezza.

2. La responsabilità di determinare la "necessità di sapere" spetta all'SGC, agli organismi decentrati dell'UE e al servizio o dipartimento dello Stato membro presso cui la persona in questione sarà assunta, in funzione dei requisiti delle sue funzioni.

3. Il rilascio del nulla osta di sicurezza al personale spetta al datore di lavoro del funzionario in base alle pertinenti procedure applicabili. Per quanto riguarda i funzionari e altri agenti dell'SGC, la procedura relativa al rilascio del nulla osta di sicurezza è specificata nella sezione VI. Tale procedura si conclude con il rilascio di un "nulla osta di sicurezza" in cui è specificato il grado delle informazioni classificate cui la persona abilitata ha accesso e la data di scadenza di tale nulla osta. Un nulla osta di sicurezza per un determinato grado può conferire al titolare il diritto all'accesso ad informazioni classificate di grado inferiore.

4. Le persone che non sono funzionari o altri agenti dell'SGC o degli Stati membri, ad esempio membri, funzionari o agenti delle istituzioni dell'UE, con cui possa essere necessario discutere informazioni classificate UE, o ai quali tali informazioni devono essere mostrate, devono avere un nulla osta di sicurezza per le informazioni classificate UE e devono venir istruite quanto alla loro responsabilità in materia di sicurezza. La stessa regola si applica, in circostanze analoghe, a contraenti, esperti o consulenti esterni.

REGOLE SPECIFICHE RELATIVE ALL'ACCESSO ALLE INFORMAZIONI TRES SECRET UE/EU TOP SECRET (EU segretissimo)

5. La persona che deve accedere alle informazioni TRES SECRET UE/EU TOP SECRET (UE segretissimo) deve preliminarmente essere abilitata a tale accesso.

6. La persona che deve accedere alle informazioni TRES SECRET UE/EU TOP SECRET (UE segretissimo) è designata dal capo del servizio da cui dipende e il suo nominativo è inserito nel pertinente registro TRES SECRET UE/EU TOP SECRET (UE segretissimo).

7. Prima di accedere alle informazioni TRES SECRET UE/EU TOP SECRET (UE segretissimo) la persona in questione deve firmare un certificato in cui dichiara di essere stata istruita sulle procedure del Consiglio in materia di sicurezza e di essere pienamente consapevole della responsabilità che le incombe quanto alla protezione delle informazioni TRES SECRET UE /EU TOP SECRET (UE segretissimo) nonché delle conseguenze previste dalle norme dell'UE e dalle norme nazionali o amministrative qualora informazioni classificate vengano divulgate a persone non autorizzate, sia intenzionalmente che per negligenza.

8. Per le persone che hanno accesso a informazioni TRES SECRET UE/EU TOP SECRET (UE segretissimo) nel corso di riunioni, ecc., il funzionario di controllo competente del servizio o dell'organismo presso cui tali persone sono assunte notifica all'organo che organizza la riunione che le persone in questione sono in possesso della pertinente autorizzazione.

9. Il nominativo della persona che cessi di svolgere funzioni per le quali è richiesto l'accesso alle informazioni TRES SECRET UE/EU TOP SECRET (UE segretissimo) è rimosso dall'elenco TRES SECRET UE/EU TOP SECRET (UE segretissimo). Inoltre, la sua attenzione è nuovamente richiamata sulla responsabilità particolare che le incombe quanto alla protezione delle informazioni TRES SECRET UE/EU TOP SECRET (UE segretissimo). Essa è anche tenuta a firmare una dichiarazione in cui si impegna a non utilizzare o divulgare le informazioni TRES SECRET UE/EU TOP SECRET (UE segretissimo) in suo possesso.

REGOLE SPECIFICHE RELATIVE ALL'ACCESSO ALLE INFORMAZIONI SECRET UE (UE segreto) e CONFIDENTIEL UE (UE riservatissimo)

10. La persona che deve accedere alle informazioni SECRET UE (UE segreto) e CONFIDENTIEL UE (UE riservatissimo) deve essere preliminarmente abilitata al pertinente grado.

11. La persona che deve accedere alle informazioni SECRET UE (UE segreto) e CONFIDENTIEL UE (UE riservatissimo) deve essere a conoscenza delle pertinenti norme di sicurezza ed essere consapevole delle conseguenze di un atto di negligenza.

12. Per le persone che hanno accesso a informazioni SECRET UE (UE segreto) e CONFIDENTIEL UE (UE riservatissimo) nel corso di riunioni, ecc., il capo della sicurezza del servizio o dell'organismo presso cui tali persone sono assunte notifica all'organismo che organizza la riunione che le persone in questione sono in possesso della pertinente autorizzazione.

REGOLE SPECIFICHE RELATIVE ALL'ACCESSO ALLE INFORMAZIONI RESTREINT UE (UE riservato)

13. La persona che ha accesso a informazioni RESTREINT UE (UE riservato) viene messa a conoscenza delle presenti norme di sicurezza e delle conseguenze di un atto di negligenza.

TRASFERIMENTI

14. Quando un membro del personale è trasferito da un posto che comporta il trattamento di materiale classificato UE, l'ufficio della registrazione provvede al corretto trasferimento di detto materiale dal funzionario uscente al funzionario entrante.

ISTRUZIONI PARTICOLARI

15. La persona che deve trattare informazioni classificate UE deve essere resa consapevole, all'atto dell'assunzione delle sue funzioni e successivamente con periodicità, di quanto segue:

    a) i pericoli per la sicurezza derivanti da conversazioni indiscrete;

    b) le precauzioni da prendere nei rapporti con la stampa;

    c) la minaccia rappresentata dalle attività di servizi segreti che prendono di mira l'UE e gli Stati membri per quanto riguarda le informazioni e le attività classificate UE;

    d) l'obbligo di riferire immediatamente alle pertinenti autorità di sicurezza in merito a qualsiasi approccio o manovra che possa destare i sospetti di un'attività di spionaggio o di qualsiasi circostanza inabituale in materia di sicurezza.

16. Tutti coloro che sono abitualmente esposti a frequenti contatti con rappresentanti di paesi i cui servizi segreti prendono di mira l'UE e gli Stati membri per quanto riguarda le informazioni e le attività classificate UE vengono istruiti sulle tecniche notoriamente impiegate dai vari servizi segreti.

17. Non esistono norme di sicurezza del Consiglio relative ai viaggi personali verso qualsiasi destinazione effettuati da personale abilitato all'accesso a informazioni classificate UE. Le pertinenti autorità di sicurezza, tuttavia, informano i funzionari e altri agenti di cui sono responsabili in merito alle disposizioni in materia di viaggio cui possono essere soggetti. Spetta ai responsabili della sicurezza organizzare riunioni di aggiornamento per i membri del personale su queste istruzioni particolari.

SEZIONE VI

PROCEDURA PER IL RILASCIO DEL NULLA OSTA DI SICUREZZA AI FUNZIONARI E ALTRI AGENTI DELL'SGC

1. Hanno accesso alle informazioni classificate in possesso del Consiglio soltanto i funzionari e gli altri agenti dell'SGC o le persone che lavorano in seno all'SGC che, a motivo delle loro funzioni e per esigenze di servizio, abbiano bisogno di prenderne visione o di effettuarne il trattamento.

2. Per poter accedere alle informazioni classificate TRES SECRET UE/EU TOP SECRET (UE segretissimo), SECRET UE (UE segreto) e CONFIDENTIEL UE (UE riservatissimo) le persone di cui al punto 1 devono essere state abilitate a tal fine, secondo la procedura di cui ai paragrafi 4 e 5.

3. Il nulla osta di sicurezza è rilasciato soltanto alle persone che sono state oggetto di un'indagine di sicurezza da parte delle autorità nazionali competenti degli Stati membri (NSA) secondo la procedura di cui ai paragrafi da 6 a 10.

4. L'autorità che ha il potere di nomina (APN) ai sensi dell'articolo 2, primo comma, dello statuto è competente per il rilascio del nulla osta di sicurezza di cui ai paragrafi 1, 2 e 3.

   L'APN rilascia tale nulla osta previo parere delle autorità nazionali competenti degli Stati membri sulla base dell'indagine di sicurezza condotta ai sensi dei paragrafi da 6 a 12.

5. Il nulla osta di sicurezza, che è valido per un periodo di cinque anni, non può avere durata superiore a quella delle funzioni che ne hanno giustificato il rilascio. Esso può essere rinnovato dall'APN secondo la procedura di cui al paragrafo 4.

   Il nulla osta di sicurezza è revocato dall'APN ove questa ritenga che ve ne sia motivo. La decisione di revoca è notificata alla persona interessata, che può chiedere di essere ascoltata dall'APN, nonché all'autorità nazionale competente.

6. L'indagine di sicurezza ha lo scopo di assicurare che nulla osti a che la persona possa avere accesso alle informazioni classificate in possesso del Consiglio.

7. L'indagine di sicurezza è effettuata, con la collaborazione della persona interessata e su richiesta dell'APN, dalle autorità nazionali competenti dello Stato membro di cui la persona da abilitare è cittadino. Qualora la persona interessata risieda nel territorio di un altro Stato membro, le autorità nazionali competenti possono avvalersi della collaborazione delle autorità dello Stato di residenza.

8. Ai fini dell'indagine la persona interessata è tenuta a compilare una nota informativa individuale.

9. Nella richiesta l'APN specifica il tipo e il grado di classificazione delle informazioni di cui la persona interessata dovrà prendere visione, per consentire alle autorità nazionali competenti di svolgere l'indagine ed esprimere un parere per il grado di abilitazione appropriato da rilasciare alla persona in questione.

10. Per lo svolgimento e i risultati della procedura relativa all'indagine di sicurezza sono applicabili le disposizioni e le norme vigenti in materia nello Stato membro interessato, comprese quelle relative agli eventuali mezzi di impugnazione.

11. Se le autorità nazionali competenti degli Stati membri esprimono parere positivo, l'APN può rilasciare il nulla osta alla persona interessata.

12. Se le autorità nazionali competenti esprimono parere negativo, la persona interessata è informata di tale parere e può chiedere di essere ascoltata dall'APN. L'APN può, se lo ritiene necessario, rivolgersi alle autorità nazionali competenti per chiedere i chiarimenti complementari che esse sono in grado di fornire. In caso di riconferma del parere negativo, il nulla osta non può essere rilasciato.

13. Ogni persona abilitata a norma dei paragrafi 4 e 5 riceve, al momento del rilascio del nulla osta e successivamente ad intervalli regolari, le necessarie istruzioni concernenti la protezione delle informazioni classificate e le modalità per garantirla. Essa firma una dichiarazione in cui conferma di avere ricevuto tali istruzioni e di impegnarsi a rispettarle.

14. L'APN adotta le misure necessarie per attuare la presente sezione, in particolare per quanto riguarda le norme in materia di accesso all'elenco delle persone abilitate.

15. In via eccezionale e per esigenze di servizio l'APN, previa informazione delle autorità nazionali competenti e in mancanza di reazioni da parte di queste ultime entro il termine di un mese, può rilasciare un nulla osta a titolo temporaneo per un periodo che non può essere superiore a sei mesi, in attesa dell'esito dell'indagine di cui al paragrafo 7.

16. I nulla osta provvisori e temporanei rilasciati non danno accesso alle informazioni TRES SECRET UE/EU TOP SECRET (UE segretissimo); tale accesso è limitato ai funzionari che siano stati effettivamente sottoposti a un'indagine di sicurezza con esito positivo, ai sensi del paragrafo 7. In attesa dell'esito dell'indagine, i funzionari per i quali è stato richiesto un nulla osta di sicurezza al grado di TRES SECRET UE/EU TOP SECRET (UE segretissimo) possono essere abilitati in via temporanea e provvisoria ad accedere a informazioni classificate fino al grado TRES SECRET UE/EU TOP SECRET (UE segretissimo) incluso.

SEZIONE VII

ELABORAZIONE, DISTRIBUZIONE, TRASMISSIONE, ARCHIVIAZIONE E DISTRUZIONE DI MATERIALE CLASSIFICATO UE

Indice

Disposizioni generali

La presente sezione precisa le misure per l'elaborazione, la distribuzione, la trasmissione, l'archiviazione e la distruzione di documenti classificati UE, secondo quanto definito al paragrafo 3, lettera a) dei principi fondamentali e norme minime di sicurezza di cui alla parte I del presente allegato. Va utilizzata come riferimento per adeguare dette misure ad altro materiale classificato UE, in base al tipo e in funzione dei singoli casi.

Capitolo I

Elaborazione e distribuzione di documenti classificati UE

ELABORAZIONE

1. Le classificazioni e i contrassegni UE sono applicati secondo le disposizioni della sezione II e figurano sulla parte superiore e inferiore di ogni pagina, al centro. Ogni pagina è numerata. Ciascun documento classificato UE reca un numero di riferimento e una data. Nei documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) e SECRET UE (UE segreto) il numero di riferimento figura su ciascuna pagina. Qualora i documenti siano distribuiti in più esemplari ognuno di essi reca un numero di copia che figura sulla prima pagina, a fianco del numero totale di pagine. Tutti gli allegati e il materiale accluso sono elencati sulla prima pagina dei documenti classificati CONFIDENTIEL UE (UE riservatissimo) o di grado superiore.

2. I documenti classificati CONFIDENTIEL UE (UE riservatissimo) o di grado superiore sono dattiloscritti, tradotti, archiviati, fotocopiati, riprodotti su supporto magnetico o microfilm soltanto da persone che hanno ricevuto il nulla osta di sicurezza per l'accesso alle informazioni classificate UE per un grado almeno pari alla classificazione di sicurezza del documento in questione, ad eccezione del caso particolare di cui al paragrafo 27 della presente sezione.

   Le disposizioni che disciplinano la produzione informatica di documenti classificati sono riportate nella sezione XI.

DISTRIBUZIONE

3. Le informazioni classificate UE sono distribuite solo alle persone aventi necessità di sapere e che hanno ricevuto il pertinente nulla osta di sicurezza. La distribuzione iniziale è specificata dall'originatore.

4. I documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) sono distribuiti tramite gli uffici di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo) (cfr. la sezione VIII). Per i messaggi TRES SECRET UE/EU TOP SECRET (UE segretissimo) l'ufficio di registrazione competente può autorizzare il capo del centro di comunicazioni a produrre il numero di copie specificato nell'elenco dei destinatari.

5. I documenti classificati SECRET UE (UE segreto) o di grado inferiore possono essere ridistribuiti dal destinatario originale ad altri destinatari in base alla necessità di sapere. Le autorità d'origine tuttavia indicano chiaramente ogni limitazione che desiderino imporre. In presenza di tali limitazioni i destinatari possono ridistribuire i documenti solo con l'autorizzazione dell'autorità d'origine.

6. Ogni documento classificato CONFIDENTIEL UE (UE riservatissimo) o di grado superiore viene registrato, all'entrata e all'uscita dall'edificio, dall'ufficio di registrazione interno. I dettagli da annotare (riferimenti, data e, ove applicabile, numero della copia) sono tali da consentire l'identificazione dei documenti e sono iscritti in un repertorio o registrati su un supporto informatico specificamente protetto.

Capitolo II

Trasmissione di documenti classificati UE

INVOLUCRI

7. I documenti classificati CONFIDENTIEL UE (UE riservatissimo) o di grado superiore sono trasmessi in buste doppie, resistenti, opache. La busta interna reca la pertinente classificazione di sicurezza UE e, ove possibile, i dati completi della funzione, del titolo e dell'indirizzo del destinatario.

8. Solo il funzionario di controllo dell'ufficio di registrazione, o il suo sostituto, può aprire la busta interna e accusare ricevuta dei documenti che contiene a meno che essa sia indirizzata ad una persona determinata; in tal caso il pertinente ufficio di registrazione registra l'entrata della busta e soltanto la persona cui essa è indirizzata può aprire la busta interna e accusare ricevuta dei documenti in essa contenuti.

9. Nella busta interna viene inserito un modulo di ricevuta, che non viene classificato, indicante il numero di riferimento, la data e il numero di copia del documento ma in nessun caso l'oggetto del contenuto.

10. La busta interna è inserita in una busta esterna recante un numero di involucro ai fini della ricevuta. In nessun caso la busta esterna reca la classificazione di sicurezza.

11. Per i documenti classificati CONFIDENTIEL UE (UE riservatissimo) o di grado superiore, viene consegnata ai corrieri una ricevuta con il numero di involucro.

TRASMISSIONE ALL'INTERNO DI UN EDIFICIO O DI UN GRUPPO DI EDIFICI

12. All'interno di un determinato edificio o gruppo di edifici, i documenti classificati possono essere trasportati in una busta sigillata recante unicamente il nome del destinatario, purché il trasporto sia effettuato materialmente da una persona abilitata al grado di classificazione dei documenti.

TRASMISSIONE DI DOCUMENTI UE ALL'INTERNO DI UN PAESE

13. All'interno di un paese i documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) devono essere inviati solo a mezzo di un servizio ufficiale di messaggeria o tramite persone abilitate ad accedere a informazioni TRES SECRET UE/EU TOP SECRET (UE segretissimo).

14. Per il ricorso a un servizio di messaggeria in caso di trasmissione di un documento TRES SECRET UE/EU TOP SECRET (UE segretissimo) al di fuori di un edificio o di un gruppo di edifici, devono essere rispettate le disposizioni relative all'involucro e alla ricezione di cui al presente capitolo. L'organico dei servizi di messaggeria è tale da garantire che gli involucri contenenti documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) siano in ogni momento sotto la supervisione diretta di un funzionario responsabile.

15. In via eccezionale i documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) possono essere trasportati da funzionari, non appartenenti a un servizio di messaggeria, al di fuori di un edificio o gruppo di edifici per la loro utilizzazione in loco nel corso di riunioni o discussioni, purché:

    a) il latore sia abilitato ad accedere a tali documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo);

    b) il modo di trasporto sia conforme alle norme nazionali che disciplinano la trasmissione di documenti nazionali TOP SECRET (segretissimo);

    c) in nessuna circostanza i documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) siano lasciati incustoditi;

    d) si definiscano procedure affinché l'elenco dei documenti trasportati in tal modo sia iscritto presso l'ufficio di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo) che detiene i documenti e in un apposito repertorio e sia ricontrollato all'atto della riconsegna.

16. All'interno di un paese i documenti SECRET UE (UE segreto) e CONFIDENTIEL UE (UE riservatissimo) possono essere spediti sia tramite posta, se tale tipo di trasmissione è consentita in base alle norme nazionali ed è conforme a dette norme, o mediante servizio di messaggeria oppure affidandoli a persone abilitate all'accesso alle informazioni classificate UE.

17. Ciascuno Stato membro, o organismo decentrato dell'UE, elabora istruzioni per il personale che trasporta documenti classificati UE in base alle presenti norme. Il datore è tenuto a leggere e firmare tali istruzioni le quali prevedono, in particolare, che in nessun caso i documenti:

    a) siano lasciati incustoditi a meno che siano conservati in modo sicuro ai sensi delle disposizioni di cui alla sezione IV;

    b) siano lasciati incustoditi su mezzi di trasporto pubblico o all'interno di veicoli privati, o in luoghi quali ristoranti o alberghi. Essi non possono essere depositati nella cassaforte degli alberghi o restare incustoditi nelle camere;

    c) siano letti in luoghi pubblici quali aeromobili o treni.

TRASMISSIONE TRA STATI MEMBRI

18. Il materiale classificato CONFIDENTIEL UE (UE riservatissimo) o di grado superiore è trasferito da uno Stato membro ad un altro mediante valigia diplomatica o corriere militare.

19. Tuttavia il trasporto personale di materiale classificato SECRET UE (UE segreto) e CONFIDENTIEL UE (UE riservatissimo) è consentito se le disposizioni per il trasporto sono tali da garantire che detto materiale non possa cadere nelle mani di persone non autorizzate.

20. Le NSA possono autorizzare il trasporto personale quando la valigia diplomatica e il corriere militare non siano disponibili o quando il ricorso a tali mezzi di trasporto comporti un ritardo che sarebbe dannoso per le operazioni dell'UE nonché quando il materiale sia richiesto urgentemente dal destinatario previsto. Ciascuno Stato membro prepara istruzioni per il trasporto personale internazionale di materiale classificato fino al grado di SECRET UE (UE segreto) incluso, effettuato da persone che non siano corrieri diplomatici o militari. Ai sensi di tali istruzioni:

   a) il latore deve avere il pertinente nulla osta di sicurezza rilasciato dagli Stati membri;

   b) il materiale trasportato è registrato nel pertinente ufficio o ufficio di registrazione;

   c) gli involucri o i plichi contenenti materiale UE recano un sigillo ufficiale volto ad evitare o scoraggiare un'ispezione doganale e etichette relative all'identificazione nonché istruzioni per chi ritrova il materiale;

   d) il latore dispone di un certificato di corriere e/o di un ordine di missione, riconosciuto da tutti gli Stati dell'UE, che lo autorizza a trasportare l'involucro specificato;

   e) in caso di viaggio via terra non viene attraversato alcun paese terzo, né la sua frontiera, a meno che lo Stato di invio non abbia una garanzia speciale da parte del paese in questione;

   f) l'organizzazione del viaggio del latore per quanto concerne destinazioni, percorsi e mezzi di trasporto è conforme alle norme dell'UE o alle norme nazionali in materia qualora queste siano più rigorose;

   g) il materiale deve sempre essere detenuto dal latore a meno che sia custodito ai sensi delle disposizioni relative alla conservazione in luogo sicuro di cui alla sezione IV;

   h) il materiale non deve essere lasciato incustodito in veicoli pubblici o privati o in luoghi quali ristoranti o alberghi. Esso non deve essere depositato nella cassaforte degli alberghi o restare incustodito nelle camere;

   i) se il materiale trasportato contiene documenti questi non devono essere letti in luoghi pubblici (ad esempio aerei, treni, ecc.).

   La persona addetta al trasporto dei documenti classificati deve leggere e firmare un documento del servizio di sicurezza in cui figurino almeno le istruzioni di cui sopra e le procedure da seguire in caso di emergenza o qualora il plico contenente il materiale classificato sia richiesto per accertamenti dai servizi doganali o di sicurezza degli aeroporti.

TRASMISSIONE DI DOCUMENTI RESTREINT UE (UE riservato)

21. Non sono previste disposizioni speciali per il trasporto di documenti RESTREINT UE (UE riservato) eccetto per quanto riguarda la garanzia che non cadano nelle mani di persone non autorizzate.

SICUREZZA DEL PERSONALE DEI CORRIERI

22. Tutto il personale del servizio di corriere e di messaggeria assunto per trasportare documenti SECRET UE (UE segreto) e CONFIDENTIEL UE (UE riservatissimo) deve essere in possesso del pertinente nulla osta di sicurezza.

Capitolo III

Trasmissione elettrica e altri mezzi di trasmissione tecnica

23. Le misure di sicurezza delle comunicazioni sono destinate a garantire la trasmissione sicura delle informazioni classificate UE. Le norme particolareggiate applicabili alla trasmissione di tali informazioni classificate UE figurano nella sezione XI.

24. Le informazioni classificate CONFIDENTIEL UE (UE riservatissimo) e SECRET UE (UE segreto) possono transitare solo attraverso centri e reti di comunicazione e/o terminali e sistemi accreditati.

Capitolo IV

Esemplari supplementari, traduzioni ed estratti di documenti classificati UE

25. Solo l'originatore può autorizzare la tiratura o la traduzione di documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo).

26. Se persone che non hanno il nulla osta di sicurezza del grado TRES SECRET UE/EU TOP SECRET (UE segretissimo) richiedono informazioni le quali, sebbene contenute in un documento TRES SECRET UE/EU TOP SECRET (UE segretissimo) non hanno tale grado di classificazione, il capo dell'ufficio di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo) può essere autorizzato a produrre il numero necessario di estratti dal documento in questione. Contemporaneamente egli adotta le misure necessarie affinché a tali estratti venga attribuita la pertinente classificazione di sicurezza.

27. I documenti classificati SECRET UE (UE segreto) o di grado inferiore possono essere riprodotti e tradotti dal destinatario nell'ambito delle norme nazionali in materia di sicurezza e purché sia rigorosamente rispettato il principio della necessità di sapere. Le misure di sicurezza applicabili al documento originale si applicano anche alle riproduzioni e/o traduzioni del medesimo. Gli organismi decentrati dell'UE applicano le presenti norme di sicurezza.

Capitolo V

Rassegne e controlli, archiviazione e distruzione dei documenti classificati UE

RASSEGNE E CONTROLLI

28. Ogni anno l'ufficio di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo), di cui alla sezione VIII, effettua una rassegna particolareggiata dei documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) conformemente alle disposizioni previste alla sezione VIII, paragrafi da 9 a 11. I documenti classificati UE di grado inferiore a TRES SECRET UE/EU TOP SECRET (UE segretissimo) sono soggetti a controlli interni in funzione di orientamenti nazionali e, per l'SGC o gli organismi decentrati dell'UE, in base a istruzioni del Segretario generale/Alto rappresentante.

    Tali operazioni mirano ad ottenere il parere dei detentori dei documenti quanto:

    a) alla possibilità di declassare o declassificare determinati documenti;

    b) ai documenti da distruggere.

ARCHIVIAZIONE DELLE INFORMAZIONI CLASSIFICATE UE

29. Al fine di ridurre al minimo i problemi di archiviazione, i funzionari di controllo di tutti gli uffici di registrazione sono autorizzati a far microfilmare i documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo), SECRET UE (UE segreto) e CONFIDENTIEL UE (UE riservatissimo) o a farli riprodurre su supporto magnetico o ottico a fini di archiviazione, purché:

    a) il processo di trasferimento su microfilm/di archiviazione sia effettuato da personale con nulla osta valido per il corrispondente grado di classificazione;

    b) il microfilm/mezzo di archiviazione goda della stessa sicurezza dei documenti originali;

    c) il trasferimento su microfilm/l'archiviazione di ogni documento TRES SECRET UE/EU TOP SECRET (UE segretissimo) sia comunicato all'originatore;

d) i rotoli di pellicola, o gli altri tipi di supporto, contengano solo documenti del medesimo grado di classificazione TRES SECRET UE/EU TOP SECRET (UE segretissimo), SECRET UE (UE segreto) e CONFIDENTIEL UE (UE riservatissimo);

e) il trasferimento su microfilm/l'archiviazione di un documento TRES SECRET UE/EU TOP SECRET (UE segretissimo) o SECRET UE (UE segreto) sia chiaramente indicato nel registro usato per l'inventario annuale;

f) i documenti originali che sono stati trasferiti su microfilm o archiviati in altro modo siano distrutti, conformemente alle disposizioni di cui ai paragrafi da 31 a 36.

30. Queste norme si applicano altresì a qualsiasi altra forma di archiviazione autorizzata dalle NSA, quali i mezzi elettromagnetici e i dischi ottici.

DISTRUZIONE PERIODICA DEI DOCUMENTI CLASSIFICATI UE

31. Per evitare l'accumulazione superflua di documenti classificati UE, gli esemplari che il capo dell'istituzione che li detiene considera superati o in soprannumero sono distrutti non appena possibile, nel seguente modo:

a) i documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) sono distrutti soltanto dall'ufficio centrale di registrazione che ne è responsabile. Ogni documento distrutto viene elencato in un certificato di distruzione, firmato dal funzionario di controllo TRES SECRET UE/EU TOP SECRET (UE segretissimo) e dal funzionario che assiste alla distruzione il quale deve avere il nulla osta di sicurezza di grado TRES SECRET UE/EU TOP SECRET (UE segretissimo). A tal fine nel repertorio viene inserita una nota.

b) L'ufficio di registrazione tiene i certificati di distruzione, unitamente alle schede di distribuzione, per un periodo di dieci anni e ne invia copie all'originatore o al pertinente ufficio centrale di registrazione solo su richiesta esplicita.

c) I documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) inclusi quelli classificati e poi scartati nella fase di preparazione quali copie rovinate, bozze di lavoro, note dattiloscritte e copie su carta carbone sono, sotto la sorveglianza di un funzionario TRES SECRET UE/EU TOP SECRET (UE segretissimo) distrutti mediante incenerimento, ridotti in pasta, sminuzzati o altrimenti ridotti in una forma irriconoscibile e non ricostituibile.

32. I documenti SECRET UE (UE segreto) sono distrutti dall'ufficio di registrazione che ne è responsabile, sotto la sorveglianza di una persona con nulla osta di sicurezza, utilizzando uno dei processi di cui al paragrafo 31, lettera c). I documenti SECRET UE (UE segreto) distrutti sono elencati in un certificato di distruzione firmato, detenuto dall'ufficio di registrazione, unitamente alle schede di distribuzione, per almeno tre anni.

33. I documenti CONFIDENTIEL UE (UE riservatissimo) sono distrutti dall'ufficio di registrazione che ne è responsabile, sotto la sorveglianza di una persona con nulla osta di sicurezza, utilizzando uno dei processi di cui al paragrafo 31, lettera c). La loro distruzione è registrata conformemente alle norme nazionali e, per l'SGC e gli organismi decentrati dell'UE, in base a istruzioni del Segretario generale/Alto rappresentante.

34. I documenti RESTREINT UE (UE riservato) sono distrutti dall'ufficio di registrazione che ne è responsabile o dall'utente, conformemente alle norme nazionali e, per l'SGC e gli organismi decentrati dell'UE, in base a istruzioni del Segretario generale/Alto rappresentante.

DISTRUZIONE IN SITUAZIONI DI EMERGENZA

35. L'SGC, gli Stati membri e gli organismi decentrati dell'UE predispongono piani, in base alle condizioni vigenti in loco, per la protezione del materiale classificato UE in situazioni di crisi, compresa, se necessaria, la distruzione di emergenza e piani di evacuazione; essi emanano, nell'ambito delle rispettive organizzazioni, le istruzioni che ritengono necessarie per impedire che informazioni classificate dell'UE cadano nelle mani di persone non autorizzate.

36. Le disposizioni per la protezione e/o la distruzione di materiale SECRET UE (UE segreto) e CONFIDENTIEL UE (UE riservatissimo) in situazioni di crisi non compromette in alcun modo la protezione o la distruzione di materiale TRES SECRET UE/EU TOP SECRET (UE segretissimo), ivi compresa l'attrezzatura di cifratura, il cui trattamento è prioritario rispetto a tutte le altre funzioni. Le misure da adottare per la protezione e la distruzione dell'attrezzatura di cifratura in situazioni di emergenza sono contenute in istruzioni ad hoc.

Capitolo VI

Norme specifiche applicabili ai documenti destinati al Consiglio

37. Nell'ambito dell'SGC un "Ufficio per le informazioni classificate" controlla le informazioni classificate SECRET UE (UE segreto) e CONFIDENTIEL UE (UE riservatissimo) contenute nei documenti destinati al Consiglio.

    Sotto l'autorità del Direttore generale del personale e dell'amministrazione, tale ufficio:

    a) gestisce le operazioni relative alla registrazione, riproduzione, traduzione, trasmissione, spedizione e distruzione di tali informazioni;

    b) aggiorna l'elenco dei dati relativi alle informazioni classificate;

    c) periodicamente interroga gli emittenti sulla necessità di mantenere la classificazione delle informazioni;

    d) stabilisce, di concerto con il servizio di sicurezza, le modalità pratiche per la classificazione e la declassificazione delle informazioni.

38. L'Ufficio per le informazioni classificate tiene un registro con i seguenti dati:

    a) data di elaborazione delle informazioni classificate;

    b) grado di classificazione;

    c) data di scadenza della classificazione;

    d) nome e servizio dell'originatore;

    e) destinatario o destinatari con numero di serie;

    f) oggetto;

    g) numero;

    h) numero di esemplari distribuiti;

    i) preparazione di inventari delle informazioni classificate sottoposte al Consiglio;

    j) registro della declassificazione o declassamento delle informazioni classificate.

39. Le norme generali previste nei capitoli da I a V della presente sezione si applicano all'Ufficio per le informazioni classificate dell'SGC, salvo altrimenti previsto da norme specifiche nel presente capitolo.

SEZIONE VIII

UFFICI DI REGISTRAZIONE TRES SECRET UE/EU TOP SECRET (UE segretissimo)

1. Scopo degli uffici di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo) è quello di assicurare che i documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) siano registrati, trattati e diffusi conformemente alle norme di sicurezza. Il capo dell'ufficio di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo) in ciascuno Stato membro, presso l'SGC e, se del caso, presso gli organismi decentrati delle UE, è il funzionario di controllo TRES SECRET UE/EU TOP SECRET (UE segretissimo).
2. Negli Stati membri, presso l'SGC e gli organismi decentrati dell'UE in cui siano stati istituiti siffatti registri e, se del caso, presso altre istituzioni dell'UE ed organizzazioni internazionali e nei paesi terzi con cui il Consiglio ha concluso accordi sulle procedure di sicurezza per lo scambio di informazioni classificate gli uffici centrali di registrazione sono la principale autorità preposta alla ricezione e all'invio.
3. Se necessario sono istituite sottosezioni degli uffici di registrazione per la gestione interna dei documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo); tali sottosezioni dispongono di dati aggiornati relativi alla circolazione di ciascun documento di loro competenza.
4. Le sottosezioni degli uffici di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo) sono istituite secondo quanto specificato nella sezione I per far fronte ad esigenze a lungo termine e sono aggregate ad un ufficio centrale di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo). Qualora debbano essere consultati solo in via temporanea o occasionale, i documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) possono essere rilasciati senza istituire una sottosezione TRES SECRET UE/EU TOP SECRET (UE segretissimo), purché vengano stabilite norme atte a garantire che essi rimangano sotto il controllo del competente ufficio di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo) e che siano osservate tutte le misure di sicurezza materiali e relative al personale.
5. Le sottosezioni degli uffici di registrazione non possono trasmettere documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) direttamente ad altre sottosezioni dello stesso ufficio centrale di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo) senza l'esplicito accordo di quest'ultimo.
6. Tutti gli scambi di documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) fra sottosezioni non aggregate ad uno stesso ufficio centrale di registrazione avvengono tramite gli uffici centrali di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo).

UFFICI CENTRALI DI REGISTRAZIONE TRES SECRET UE/EU TOP SECRET (UE segretissimo)

7. In qualità di funzionario di controllo, il capo di un ufficio centrale di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo) è responsabile di quanto segue:
   a) trasmissione di documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) conformemente alle norme di cui alla sezione VII;
   b) compilazione di un elenco di tutte le sottosezioni dell'ufficio di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo) che dipendono dal suo ufficio, corredato dei nomi e delle firme dei funzionari di controllo designati e dei loro supplenti autorizzati;
   c) conservazione delle ricevute dei registri per tutti i documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) distribuiti dall'ufficio centrale di registrazione;
   d) registrazione di tutti i documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) custoditi e distribuiti;
   e) aggiornamento costante di un elenco di tutti gli uffici centrali di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo) con cui è normalmente in contatto, corredato dei nomi e delle firme dei rispettivi funzionari di controllo designati e dei loro supplenti autorizzati;
   f) protezione materiale di tutti i documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) custoditi presso l'ufficio di registrazione conformemente alle norme di cui alla sezione IV.

SOTTOSEZIONI DEGLI UFFICI DI REGISTRAZIONE TRES SECRET UE/EU TOP SECRET (UE segretissimo)

8. In qualità di funzionario di controllo, il capo di una sottosezione dell'ufficio di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo) è responsabile di quanto segue:
   a) trasmissione di documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) conformemente alle norme di cui alla sezione VII ed ai paragrafi 5 e 6 della sezione VIII;
   b) aggiornamento costante di un elenco di tutte le persone autorizzate ad accedere alle informazioni TRES SECRET UE/EU TOP SECRET (UE segretissimo) di sua competenza;

c) distribuzione di documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) secondo le istruzioni dell'originatore o in base al principio della necessità di sapere dopo avere accertato che il destinatario sia fornito del necessario nullaosta di sicurezza;

d) aggiornamento costante di un registro di tutti i documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) custodito o circolanti sotto il suo controllo o passati ad altri uffici di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo) e conservazione delle relative ricevute;

e) aggiornamento costante dell'elenco degli uffici centrali di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo) con cui è autorizzato a scambiare documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo), corredato dei nomi e delle firme dei rispettivi funzionari di controllo e dei loro supplenti autorizzati;

f) protezione materiale di tutti i documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) custoditi presso la sottosezione dell'ufficio di registrazione conformemente alle norme di cui alla sezione IV.

INVENTARI

9. Ogni dodici mesi ciascun ufficio di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo) effettua un inventario dettagliato di tutti i documenti TRES SECRET UE/EU TOP SECRET (UE segretissimo) di cui è responsabile. Un documento si considera inventariato quando l'ufficio lo detiene materialmente ovvero è in possesso della ricevuta dell'ufficio di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo) in cui il documento è stato trasferito o del certificato di distruzione del documento stesso o di istruzioni relative al suo declassamento o alla sua declassificazione.

10. Le sottosezioni degli uffici di registrazione trasmettono i risultati dell'inventario annuale all'ufficio centrale di registrazione da cui dipendono in data stabilita da detto ufficio.

11. Le NSA e le istituzioni UE, le organizzazioni internazionali e gli organismi decentrati dell'UE in cui sia stato istituito un ufficio centrale di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo) trasmettono i risultati degli inventari annuali effettuati presso gli uffici centrali di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo) al Segretario generale/Alto rappresentante entro il 1 o aprile di ciascun anno.

SEZIONE IX

MISURE DI SICUREZZA DA APPLICARE IN OCCASIONE DI RIUNIONI SPECIFICHE TENUTE FUORI DEI LOCALI DEL CONSIGLIO E CONCERNENTI QUESTIONI ALTAMENTE SENSIBILI

CONSIDERAZIONI GENERALI

1. Quando riunioni del Consiglio europeo, sessioni del Consiglio, riunioni ministeriali o altre riunioni importanti hanno luogo fuori dei locali del Consiglio a Bruxelles o Lussemburgo ed ove le particolari esigenze di sicurezza connesse con l'elevata sensibilità delle questioni o delle informazioni discusse lo giustifichino, sono adottate le misure di sicurezza descritte in appresso. Tali misure riguardano unicamente la protezione delle informazioni classificate UE; potrebbe essere necessario prevedere altre misure di sicurezza.

RESPONSABILITA'

Stati membri ospitanti

2. Lo Stato membro sul cui territorio si svolge la riunione (Stato membro ospitante) è responsabile, in collaborazione con il Servizio di sicurezza dell'SGC, della sicurezza delle riunioni del Consiglio europeo, delle sessioni del Consiglio, delle riunioni ministeriali o di altre riunioni importanti, nonché della sicurezza fisica dei principali delegati e del loro seguito.

   Per quanto riguarda la salvaguardia della sicurezza, esso provvede in particolare:

   a) all'elaborazione di piani atti a contrastare le minacce alla sicurezza e far fronte agli incidenti connessi con la sicurezza, mediante misure intese in particolare a garantire che i documenti classificati UE siano custoditi negli uffici in condizioni di sicurezza;

   b) all'adozione di misure intese a fornire una possibilità di accesso al sistema di comunicazioni del Consiglio per la ricezione e la trasmissione di messaggi classificati UE. Lo Stato membro ospitante fornisce inoltre, su richiesta, l'accesso a sistemi telefonici protetti.

Stati membri

3. Le autorità degli Stati membri prendono i provvedimenti necessari al fine di:

   a) certificare in modo appropriato il nullaosta di sicurezza dei rispettivi delegati nazionali, se necessario mediante segnalazione o via fax, direttamente al responsabile della sicurezza della riunione o tramite il Servizio di sicurezza dell'SGC;

   b) informare di eventuali specifiche minacce le autorità dello Stato membro ospitante e, se del caso, il Servizio di sicurezza dell'SGC affinché possano essere adottate misure appropriate.

Responsabile della sicurezza della riunione

4. Dovrebbe essere designato un responsabile della sicurezza competente per la preparazione generale e controllo delle misure generiche di sicurezza interna, nonché per il coordinamento con le altre autorità di sicurezza interessate. Le misure adottate dal responsabile della sicurezza sono, di norma, del seguente tipo:

   a) i) misure di protezione presso la sede della riunione onde scongiurare incidenti che potrebbero compromettere la sicurezza delle informazioni classificate UE eventualmente utilizzate nel corso della riunione;

   i) controllo del personale cui è consentito l'accesso alla sede della riunione, alle aree riservate alle delegazioni ed alle sale delle conferenze e controllo di tutte le apparecchiature;

   ii) costante coordinamento con le autorità competenti dello Stato membro ospitante e con il Servizio di sicurezza dell'SGC.

   b) inserimento nel dossier della riunione di istruzioni relative alla sicurezza, tenendo in debito conto quanto prescritto dalle presenti norme di sicurezza, e qualsiasi altra istruzione relativa alla sicurezza ritenuta necessaria.

Servizio di sicurezza dell'SGC

5. Il Servizio di sicurezza dell'SGC funge da consulente in materia di sicurezza per la preparazione della riunione ed invia in loco un suo rappresentante onde fornire, se necessario, assistenza e consulenza al responsabile della sicurezza della riunione ed alle delegazioni.

6. Ogni delegazione che prende parte ad una riunione designa un funzionario preposto alla sicurezza, incaricato di discutere con la rispettiva delegazione le questioni attinenti alla sicurezza e di mantenere i contatti con il responsabile della sicurezza della riunione e, se necessario, con il rappresentante del Servizio di sicurezza del Consiglio.

MISURE DI SICUREZZA

Zone di sicurezza

7. Sono istituite le seguenti zone di sicurezza:

   a) una zona di sicurezza di categoria II, comprendente la sala di redazione, gli uffici dell'SGC e le apparecchiature di riproduzione, nonché gli uffici delle delegazioni a seconda dei casi;

   b) una zona di sicurezza di categoria I, costituita dalla sala della conferenza e dalle cabine degli interpreti e dei tecnici audio;

   c) zone amministrative, comprendenti l'area stampa e le aree della sede della riunione utilizzate a fini amministrativi, di ristorazione e di alloggio, nonché la zona immediatamente adiacente al centro stampa ed alla sede della riunione.

Lasciapassare

8. Il responsabile della sicurezza della riunione rilascia appositi badge secondo le richieste delle delegazioni ed in base alle loro esigenze operando, se necessario, una distinzione per l'accesso alle diverse zone di sicurezza.

9. Le istruzioni di sicurezza relative alla riunione prevedono che all'interno della sede della riunione tutti gli interessati portino sempre in modo ben visibile i loro badge, affinché il personale addetto alla sicurezza possa provvedere ai necessari controlli.

10. Oltre che ai partecipanti forniti di badge, l'accesso alla sede della riunione è consentito al minor numero possibile di persone. Le delegazioni nazionali che desiderino ricevere visitatori nel corso della riunione informano il responsabile della sicurezza della riunione. Ai visitatori viene rilasciato un apposito badge, previa compilazione di lasciapassare recante il nome del visitatore e della persona visitata. I visitatori sono sempre accompagnati da una guardia di sicurezza o dalla persona visitata. L'accompagnatore porta il lasciapassare del visitatore e lo riconsegna, assieme al badge del visitatore, al personale di sicurezza quando il visitatore lascia la sede della riunione.

Controllo degli apparecchi fotografici e degli apparecchi di registrazione audiovisiva

11. Nella zona di sicurezza di categoria I è vietato introdurre apparecchi fotografici e di registrazione, ad eccezione delle apparecchiature dei fotografi e dei tecnici audio debitamente autorizzati dal responsabile della sicurezza della riunione.

Controllo di valigie, computer portatili e plichi

12. I detentori di lasciapassare cui è consentito l'accesso ad una zona di sicurezza possono di norma introdurvi senza controlli le loro valigie ed i loro computer portatili (solo autoalimentati). I plichi per le delegazioni vengono loro consegnati dopo essere stati ispezionati dal funzionario della delegazione addetto alla sicurezza, controllati mediante apparecchiature speciali o aperti dal personale addetto alla sicurezza per verificarne il contenuto. Se il responsabile della sicurezza della riunione lo ritiene necessario, si possono prevedere misure più rigorose per il controllo di valigie e plichi.

Sicurezza tecnica

13. Un'apposita squadra può garantire la sicurezza tecnica della sala di riunione e provvedere inoltre alla sorveglianza elettronica durante la riunione.

Documenti delle delegazioni

14. Le delegazioni sono responsabili dei documenti classificati UE che portano con sé alle riunioni. Sono inoltre responsabili della verifica e della sicurezza di detti documenti durante la loro utilizzazione nei locali ad esse assegnati. Per il trasporto di documenti classificati nella e dalla sede della riunione può essere chiesto l'aiuto degli Stati membri ospitanti.

Custodia dei documenti in luogo sicuro

15. Se l'SGC, la Commissione o le delegazioni non sono in grado di custodire i loro documenti classificati secondo le norme approvate, possono affidarli in busta sigillata, dietro ricevuta, al responsabile della sicurezza della riunione, che li custodisce in conformità di dette norme.

Ispezione degli uffici

16. Il responsabile della sicurezza della riunione provvede a che gli uffici dell'SGC e delle delegazioni siano ispezionati al termine di ogni giornata lavorativa per verificare che tutti i documenti classificati UE siano al sicuro; in caso contrario, adotta i provvedimenti necessari.

Eliminazione dei rifiuti classificati

17. Tutti i rifiuti sono trattati come rifiuti classificati UE, per la cui eliminazione vengono forniti all'SGC e alle delegazioni cestini o pacchi della spazzatura. Prima di lasciare i locali ad essi assegnati, l'SGC e le delegazioni portano i loro rifiuti al responsabile della sicurezza della riunione, che provvede alla loro distruzione secondo le norme.

18. Al termine della riunione tutti i documenti detenuti dall'SGC e dalle delegazioni e divenuti superflui sono trattati alla stregua di rifiuti. Prima di revocare le misure di sicurezza adottate per la riunione, viene effettuata un'accurata ispezione dei locali assegnati all'SGE ed alle delegazioni. I documenti per i quali era stata firmata una ricevuta sono distrutti, ove possibile, come prescritto alla sezione VII.

SEZIONE X

VIOLAZIONE DELLA SICUREZZA E COMPROMISSIONE DI INFORMAZIONI CLASSIFICATE UE

1. Una violazione della sicurezza è la conseguenza di atti o omissioni contrari ad una norma nazionale o del Consiglio in materia di sicurezza, che potrebbero mettere a repentaglio o compromettere informazioni classificate UE.

2. Le informazioni classificate UE sono compromesse quando esse, o parte di esse, giungono in possesso di persone non autorizzate, vale a dire sprovviste dell'appropriato nullaosta di sicurezza o che non abbiano la necessità di conoscerle, o quando è probabile che si sia verificata tale circostanza.

3. Le informazioni classificate UE possono essere compromesse per disattenzione o negligenza, a seguito di indiscrezioni o come conseguenza delle attività di servizi che prendono di mira l'UE o gli Stati membri, per quanto riguarda le loro informazioni ed attività classificate UE, ovvero di organizzazioni sovversive.

4. E' importante che tutti coloro che devono trattare informazioni classificate UE ricevano informazioni dettagliate sulle procedure di sicurezza, sui pericoli insiti nelle conversazioni indiscrete e sulle relazioni che devono intrattenere con la stampa. Essi devono essere consapevoli dell'importanza di riferire immediatamente alle autorità di sicurezza dello Stato membro, dell'istituzione o dell'organismo per cui lavorano qualsiasi violazione della sicurezza di cui vengano a conoscenza.

5. Ove un'autorità competente in materia di sicurezza riscontri o sia informata di una violazione della sicurezza relativa ad informazioni classificate UE o della perdita o della scomparsa di materiale classificato UE, adotta tempestivamente provvedimenti miranti a:

   a) accertare i fatti;

   b) valutare e limitare per quanto possibile i danni;

   c) impedire che i fatti si ripetano;

   d) informare le autorità competenti delle conseguenze della violazione della sicurezza.

   A tale scopo vengono fornite le seguenti informazioni:

   i) descrizione delle informazioni in questione, loro classificazione, numero di riferimento e numero di esemplare, data, originatore, oggetto e finalità del documento;

   ii) breve descrizione delle circostanze in cui si è verificata la violazione della sicurezza, con indicazione della data e del periodo nel quale le informazioni sono state soggette al rischio di compromissione;

   iii) se l'originatore sia stato o meno informato.

6. Non appena informata di una possibile violazione della sicurezza, ciascuna autorità di sicurezza riferisce immediatamente il fatto attenendosi alla seguente procedura: la sottosezione dell'ufficio di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo) riferisce in merito al Servizio di sicurezza dell'SGC tramite il rispettivo ufficio centrale di registrazione TRES SECRET UE/EU TOP SECRET (UE segretissimo); qualora la compromissione di informazioni classificate UE sia avvenuta nel territorio di uno Stato membro, essa viene comunicata al Servizio di sicurezza di dell'SGC come specificato al paragrafo 5 tramite il responsabile della NSA.

7. I casi riguardanti informazioni RESTREINT UE (UE riservato) devono essere riferiti solo quando presentino aspetti inconsueti.

8. Il Segretario generale/Alto rappresentante, informato di una violazione della sicurezza:

   a) ne dà notifica all'autorità d'origine dell'informazione classificata in questione;

   b) chiede alle autorità competenti in materia di sicurezza di avviare le indagini;

   c) coordina le indagini qualora sia interessata più di un'autorità competente in materia di sicurezza;

   d) fa stilare una relazione sulle circostanze della violazione, con l'indicazione della data o del periodo nel quale essa potrebbe essersi verificata ed è stata riscontrata, ed una descrizione particolareggiata del contenuto e del grado di classificazione del materiale implicato. La relazione prende in considerazione anche i danni arrecati agli interessi dell'UE o di uno o più Stati membri e le misure adottate per impedire che i fatti si ripetano.

9. L'autorità d'origine informa i destinatari ed impartisce le istruzioni del caso.

10. Chiunque sia responsabile della compromissione di informazioni classificate UE è passibile di sanzioni disciplinari in conformità delle norme e dei regolamenti pertinenti. Tali sanzioni non pregiudicano eventuali procedimenti giudiziari.

SEZIONE XI

PROTEZIONE DELLE INFORMAZIONI E DEI SISTEMI DI COMUNICAZIONE

Indice

Capitolo I

Introduzione

CONSIDERAZIONI GENERALI

1. La strategia e le prescrizioni in materia di sicurezza di cui alla presente sezione si applicano a tutti i sistemi e a tutte le reti di comunicazioni e di informazioni (in seguito SISTEMI) che trattano informazioni classificate di grado CONFIDENTIEL UE (UE riservatissimo) o grado superiore.

2. I SISTEMI che trattano informazioni RESTREINT UE (UE riservato) richiedono anche misure di sicurezza atte a proteggere la riservatezza delle informazioni. Tutti i SISTEMI richiedono misure di sicurezza atte a proteggere l'integrità e la disponibilità dei sistemi stessi e delle informazioni in essi contenute. Le misure di sicurezza da applicare a detti sistemi sono stabilite dall'autorità di accreditamento in materia di sicurezza (SAA) competente in funzione della valutazione del rischio e sono coerenti con la strategia definita dalle presenti norme di sicurezza.

3. Le misure di protezione dei sistemi di sensori con SISTEMI TI informatici incorporati sono stabilite e specificate nel contesto generale dei sistemi di cui fanno parte avvalendosi, nei limiti del possibile, delle pertinenti disposizioni della presente sezione.

MINACCE AI SISTEMI E LORO VULNERABILITA'

4. In linea generale si intende per minaccia la possibilità di una compromissione accidentale o deliberata della sicurezza. Nel caso dei SISTEMI, ciò implica la perdita di una o più delle caratteristiche di riservatezza, integrità e disponibilità. La vulnerabilità può essere definita come insufficienza o mancanza di controlli che rende più agevole o consente l'attuazione di una minaccia contro un bene o un bersaglio specifico. La vulnerabilità può derivare da un'omissione o può essere connessa con controlli non abbastanza rigorosi, completi o coerenti; può essere di natura tecnica, procedurale o funzionale.

5. Le informazioni classificate UE e non classificate trattate dai SISTEMI in forma compressa ai fini della rapidità di reperimento, comunicazione ed utilizzo sono soggette a molteplici rischi, fra cui l'accesso alle informazioni da parte di utenti non abilitati o, viceversa, l'impossibilità di accesso per gli utenti abilitati. Altri rischi sono costituiti dalla divulgazione non autorizzata e dalla contaminazione, modifica o soppressione delle informazioni. Le apparecchiature in questione, complesse ed a volta fragili, sono inoltre costose e spesso difficili da riparare o da sostituire in tempi brevi. I SISTEMI costituiscono pertanto bersagli appetibili per operazioni di raccolta di informazione e di sabotaggio, soprattutto se le misure di sicurezza sono considerate inadeguate.

MISURE DI SICUREZZA

6. Obiettivo principale delle misure di sicurezza previste nella presente sezione è offrire protezione contro la divulgazione non autorizzata di informazioni (perdita di riservatezza) e contro la perdita di integrità e di disponibilità delle informazioni. Per conseguire l'adeguata protezione di sicurezza di un SISTEMA che tratta informazioni classificate UE occorre specificare le opportune norme di sicurezza convenzionale, unitamente alle pertinenti procedure e tecniche di sicurezza speciali, progettate appositamente per ciascun SISTEMA.

7. Per creare un ambiente sicuro in cui il SISTEMA operi è istituita ed applicata una serie equilibrata di misure di sicurezza. Il campo di applicazione di tali misure riguarda gli elementi materiali, il personale, le procedure non tecniche, i computer e le procedure operative di comunicazione.

8. Le misure di sicurezza dei computer (caratteristiche di sicurezza dell'hardware e del software) sono concepite in applicazione del principio della necessità di sapere e sono atte a prevenire o a individuare la divulgazione non autorizzata di informazioni. Il grado di affidabilità delle misure di sicurezza dei computer è determinato durante la procedura di definizione dei requisiti di sicurezza. Il processo di accreditamento serve a dimostrare che sussiste un adeguato livello di certezza quanto all'affidabilità delle misure di sicurezza dei computer.

DICHIARAZIONE RELATIVA AI REQUISITI DI SICUREZZA SPECIFICI DEL SISTEMA (SSRS)

9. Per tutti i SISTEMI che trattano informazioni classificate CONFIDENTIEL UE (UE riservatissimo) o di grado superiore, l'autorità operativa del sistema TI (ITSOA) è invitata a rilasciare una dichiarazione relativa ai requisiti di sicurezza specifici del SISTEMA (SSRS), avvalendosi, ove necessario, dell'apporto e dell'assistenza del gruppo di progetto e dell'autorità INFOSEC, e con l'approvazione della SAA. Una SSRS è anche richiesta qualora la disponibilità e l'integrità delle informazioni classificate RESTREINT UE (UE riservate) o non classificate siano ritenute essenziali dalla SAA.

10. La SSRS è formulata nelle primissime fasi dell'avvio del progetto e viene sviluppata e ampliata con l'evoluzione del progetto, svolgendo differenti funzioni nelle diverse fasi del ciclo di vita del progetto e del SISTEMA.

11. La SSRS costituisce l'accordo che vincola l'autorità operativa del sistema TI e la SAA, in base al quale il SISTEMA deve essere accreditato.

12. La SSRS è una dichiarazione completa ed esplicita relativa ai principi di sicurezza da osservare e ai requisiti particolareggiati di sicurezza da rispettare. E' basato sulla politica del Consiglio in materia di sicurezza e di valutazione del rischio, oppure imposta da parametri che disciplinano l'ambiente operativo, il grado più basso di nullaosta di sicurezza del personale, il grado più alto di classificazione delle informazioni trattate, il modo di funzionamento in condizioni di sicurezza o le esigenze degli utenti. La SSRS forma parte integrante della documentazione sul progetto sottoposta alle pertinenti autorità ai fini dell'approvazione tecnica, finanziaria e di sicurezza. Nella sua forma definitiva la SSRS costituisce un elenco completo di quanto è necessario per garantire la sicurezza del SISTEMA.

FUNZIONAMENTO IN CONDIZIONI DI SICUREZZA

13. Tutti i SISTEMI che trattano informazioni classificate CONFIDENTIEL UE (UE riservatissimo) o di grado superiore sono accreditati per funzionare in uno o, ove sia giustificato dai requisiti durante diversi periodi, più di uno dei seguenti modi in condizioni di sicurezza, o equivalente nazionale:

    a) esclusivo;

    b) predominante;

    c) multilivello.

Capitolo II

Definizioni

CONTRASSEGNI SUPPLEMENTARI

14. Qualora risultino necessari una distribuzione limitata e un trattamento speciale oltre a quanto indicato dalla classificazione di sicurezza, si applicano contrassegni supplementari quali CRYPTO o qualunque altra indicazione di trattamento speciale riconosciuta a livello di UE.

15. Per FUNZIONAMENTO "ESCLUSIVO" IN CONDIZIONI DI SICUREZZA si intende un modo di funzionamento in cui TUTTE le persone che hanno accesso al SISTEMA sono in possesso di un nullaosta di sicurezza per il grado più elevato di classificazione delle informazioni trattate nel SISTEMA e con necessità di sapere comune rispetto a TUTTE le informazioni trattate nel SISTEMA.

    Note:

    1. Necessità di sapere comune

    2. Le altre caratteristiche di sicurezza (ad esempio relative al materiale, al personale o alle procedure) sono conformi ai requisiti per il grado più elevato di classificazione e per tutte le designazioni di categoria delle informazioni trattate nel SISTEMA.

16. Per FUNZIONAMENTO "PREDOMINANTE" IN CONDIZIONI DI SICUREZZA si intende un modo di funzionamento in cui TUTTE le persone che hanno accesso al SISTEMA sono in possesso di un nullaosta di sicurezza al grado più elevato di classificazione delle informazioni trattate nel SISTEMA, ma NON TUTTE le persone con accesso al SISTEMA hanno una necessità di sapere comune rispetto alle informazioni trattate nel SISTEMA.

    Note:

    1. La mancanza di una necessità di sapere comune indica che le caratteristiche di sicurezza del computer devono offrire un accesso selettivo alle informazioni nel SISTEMA e la separazione delle medesime.

    2. Le altre caratteristiche di sicurezza (ad esempio relative al materiale, al personale o alle procedure) sono conformi ai requisiti per il grado più elevato di classificazione e per tutte le designazioni di categoria delle informazioni trattate nel SISTEMA.

    3. Tutte le informazioni trattate o messe a disposizione nel SISTEMA in base a questo modo di funzionamento, unitamente all'output che ne deriva, sono protette come se rientrassero potenzialmente nella designazione di categoria e nel grado più elevato di classificazione delle informazioni trattate fino a prova contraria, a meno che sussista un livello di fiducia accettabile nei confronti della funzione di etichettatura già presente.

17. Per FUNZIONAMENTO "MULTILIVELLO" IN CONDIZIONI DI SICUREZZA si intende un modo di funzionamento in cui NON TUTTE le persone che hanno accesso al SISTEMA sono in possesso di un nullaosta di sicu-

rezza al grado più elevato di classificazione delle informazioni trattate nel SISTEMA, e NON TUTTE le persone con accesso al SISTEMA hanno una necessità di sapere comune rispetto alle informazioni trattate nel SISTEMA.

Note:

1. Questo modo di funzionamento consente attualmente il trattamento di informazioni di diversi gradi di classificazione e con diverse designazioni di categoria.
2. Il fatto che non tutte le persone siano in possesso di un nullaosta di sicurezza del grado più elevato, associato ad una mancanza di necessità di sapere comune, indica che le caratteristiche di sicurezza del computer devono offrire un accesso selettivo alle informazioni nel SISTEMA e la loro separazione.

18. Per INFOSEC si intende l'applicazione di misure di sicurezza atte a proteggere le informazioni elaborate, archiviate o trasmesse da sistemi di comunicazione, di informazione o da altri sistemi elettronici contro la perdita di riservatezza, integrità o disponibilità, accidentale o intenzionale, nonché a impedire la perdita di integrità e di disponibilità dei sistemi stessi. Le misure INFOSEC comprendono la sicurezza del computer, della trasmissione, dell'emissione e della crittografia nonché l'individuazione, la documentazione e la neutralizzazione di minacce nei confronti dell'informazione e dei SISTEMI.

19. Per SICUREZZA INFORMATICA (COMPUSEC) si intende l'applicazione a un sistema informatico di caratteristiche di sicurezza per l'hardware, il firmware e il software atte a proteggere le informazioni contro la divulgazione non autorizzata, la manipolazione, la modifica/soppressione, o a impedire tali atti, o a impedire l'interruzione di servizio.

20. Per PRODOTTO PER LA SICUREZZA INFORMATICA si intende un elemento generico per la sicurezza informatica, destinato ad essere incorporato in un sistema TI ai fini di potenziare, o di offrire, la riservatezza, l'integrità e la disponibilità delle informazioni trattate.

21. Per SICUREZZA DELLE COMUNICAZIONI (COMSEC) si intende l'applicazione di misure di sicurezza alle telecomunicazioni al fine di negare alle persone non autorizzate informazioni preziose desumibili dal possesso e dall'analisi di tali comunicazioni o di assicurare l'autenticità di tali telecomunicazioni.

Note:

Tali misure includono la sicurezza della crittografia, della trasmissione e dell'emissione nonché la sicurezza delle procedure, dei materiali, del personale, del documento e del computer.

22. Per VALUTAZIONE si intende l'esame tecnico dettagliato, da parte di un'autorità competente, degli aspetti di sicurezza di un SISTEMA o di un prodotto per la sicurezza della crittografia o del computer.

Note:

1. La valutazione accerta la presenza della funzionalità di sicurezza richiesta e l'assenza di effetti secondari compromettenti derivanti da tale funzionalità e valuta l'inalterabilità di tale funzionalità.
2. La valutazione determina se e quanto sono soddisfatti i requisiti di sicurezza di un SISTEMA, o le presunte prestazioni di sicurezza di un prodotto per la sicurezza del computer, e stabilisce il livello di attendibilità del SISTEMA o della funzione di fiducia del prodotto per la sicurezza del computer o della crittografia.

23. Per CERTIFICAZIONE si intende il rilascio di una dichiarazione ufficiale, sulla base di un esame indipendente concernente il modo in cui è stata eseguita una valutazione e i risultati che ha prodotto, che indica in quale misura un SISTEMA soddisfa il requisito di sicurezza o un prodotto per la sicurezza informatica offre le presunte prestazioni predefinite in materia di sicurezza.

24. Per ACCREDITAMENTO si intende l'autorizzazione e l'approvazione di un SISTEMA per trattare informazioni classificate UE nel suo ambiente operativo.

Note:

Tale accreditamento deve essere effettuato dopo che tutte le pertinenti procedure di sicurezza sono state attuate e una volta raggiunto un sufficiente livello di protezione delle risorse del sistema. L'accreditamento avviene di norma sulla base della SSRS e include:

a) una dichiarazione relativa all'obiettivo dell'accreditamento per il sistema, in particolare su quali gradi di classificazione delle informazioni saranno trattati e su quali modi di funzionamento in condizioni di sicurezza sono proposti per il sistema o la rete;
b) un esame sulla gestione del rischio atto a identificare le minacce e le vulnerabilità nonché le misure per contrastarle;

c) le procedure operative di sicurezza (SecOP) con una descrizione dettagliata delle operazioni proposte (ad esempio modi, servizi da fornire) e comprendenti una descrizione delle caratteristiche di sicurezza del SISTEMA su cui si basa l'accreditamento;

d) il piano per l'attuazione e la manutenzione delle caratteristiche di sicurezza;

e) il piano per il collaudo, la valutazione e la certificazione iniziali e successivi della sicurezza del sistema o della rete;

f) la certificazione, ove richiesta, unitamente ad altri elementi di accreditamento.

25. Per SISTEMA TI si intende un insieme di attrezzature, metodi e procedure e, se necessario, di personale, organizzato in modo da compiere funzioni di trattamento delle informazioni.

Note:

1. Si tratta di un insieme di strutture, configurate per trattare informazioni all'interno del sistema.
2. Tali sistemi possono essere a sostegno di applicazioni di consultazione, comando, controllo e comunicazione, di applicazioni scientifiche o amministrative, incluso il trattamento testi.
3. Un sistema è generalmente definito in base agli elementi posti sotto il controllo di un'unica ITSOA.
4. Un sistema TI può contenere sottosistemi alcuni dei quali sono essi stessi sistemi TI.

26. Le CARATTERISTICHE DI SICUREZZA DI UN SISTEMA TI comprendono tutte le funzioni e le caratteristiche hardware/firmware/software, le procedure operative, le procedure di responsabilità, i controlli di accesso, l'area TI, l'area di terminali/postazioni remoti, i vincoli della gestione, la struttura e i dispositivi materiali, i controlli del personale e delle comunicazioni necessari per fornire un livello accettabile di protezione delle informazioni classificate da trattare nel sistema TI.

27. Per RETE TI si intende l'organizzazione, geograficamente diffusa, di sistemi TI interconnessi per lo scambio di dati, comprendente i componenti dei sistemi TI interconnessi e la loro interfaccia con le reti dati o le reti di comunicazione di sostegno.

Note:

1. Una rete TI può usare i servizi di una o più reti di comunicazione interconnesse per lo scambio di dati; varie reti TI possono usare i servizi di una rete di comunicazioni comune.
2. Una rete TI è denominata "locale" se collega vari computer nel medesimo sito.

28. Le CARATTERISTICHE DI SICUREZZA DI UNA RETE TI includono le caratteristiche di sicurezza del sistema TI dei singoli sistemi che compongono la rete unitamente ai componenti e agli elementi aggiuntivi associati con la rete in quanto tale (per esempio le comunicazioni di rete, i meccanismi e le procedure per l'identificazione e l'etichettatura di sicurezza, i controlli di accesso, i programmi e gli audit trail) necessari per fornire un livello di protezione accettabile delle informazioni classificate.

29. Per AREA TI si intende un'area che contiene uno o più computer, le loro locali periferiche e unità di archiviazione, le unità di controllo e l'attrezzatura specializzate per le reti e le comunicazioni.

Note:

La definizione non include un'area separata in cui sono situati i dispositivi periferici o i terminali/postazioni remoti anche qualora detti dispositivi siano connessi all'attrezzatura collocata nell'area TI.

30. Per AREA DI TERMINALI/POSTAZIONI REMOTI si intende un'area contenente alcune attrezzature informatiche, i suoi dispositivi locali periferici o terminali/postazioni e qualsiasi attrezzatura di comunicazione associata, separata dall'area TI.

31. Per CONTROMISURE DELL'EFFETTO TEMPESTA si intendono misure di sicurezza destinate a proteggere l'attrezzatura e le infrastrutture di comunicazione contro il rischio di compromissione delle informazioni classificate dovuta a emissioni elettromagnetiche non intenzionali.

Capitolo III

Responsabilità in materia di sicurezza

DISPOSIZIONI GENERALI

32. Tra le responsabilità del Comitato per la sicurezza, di cui alla sezione I, punto 4, rientrano le questioni inerenti all'INFOSEC. Il Comitato per la sicurezza organizza le sue attività in modo da fornire una consulenza qualificata in materia.

33. In caso di problemi concernenti la sicurezza (incidenti, violazioni, ecc.) l'autorità nazionale pertinente e/o il servizio di sicurezza dell'SGC prendono misure immediate. Tutti i problemi sono sottoposti al servizio di sicurezza dell'SGC.

34. Il Segretario generale/Alto rappresentante o, ove opportuno, il Capo di un organismo decentrato dell'UE, istituisce un ufficio INFOSEC preposto a fornire orientamenti all'autorità di sicurezza circa l'attuazione e il controllo delle specifiche caratteristiche di sicurezza progettate come parti di SISTEMI.

AUTORITA' DI ACCREDITAMENTO IN MATERIA DI SICUREZZA (SAA)

35. La SAA può essere:
    - una NSA,
    - l'autorità designata dal Segretario generale/Alto rappresentante,
    - l'autorità competente in materia di sicurezza di un organismo decentrato dell'UE,
    - i rappresentanti delegati/nominati di una delle suddette autorità, in funzione del SISTEMA da accreditare.

36. La SAA è responsabile di accertare la conformità dei SISTEMI con la politica del Consiglio in materia di sicurezza. Tra i suoi compiti rientra il rilascio dell'approvazione di un SISTEMA per il trattamento delle informazioni classificate UE ad un determinato grado di classificazione nel suo ambiente operativo. Per quanto riguarda l'SGC, e se del caso gli organismi decentrati dell'UE, la SAA è responsabile della sicurezza per conto del Segretario generale/Alto rappresentante o dei capi degli organismi decentrati.

    La competenza della SAA dell'SGC si estende a tutti i SISTEMI in funzione all'interno dei locali dell'SGC. I SISTEMI e i componenti di SISTEMI in funzione presso uno Stato membro restano sotto la giurisdizione di detto Stato membro. Quando diversi componenti di un SISTEMA rientrano nella competenza della SAA dell'SGC e di altre SAA, tutte le parti nominano un comitato comune di accreditamento posto sotto il coordinamento della SAA dell'SGC.

AUTORITA' INFOSEC (IA)

37. L'autorità INFOSEC è competente per le attività dell'ufficio INFOSEC. Per quanto riguarda l'SGC, e se del caso gli organismi decentrati dell'UE, l'autorità INFOSEC è responsabile delle seguenti attività:
    - fornire consulenza e assistenza tecnica alla SAA,
    - assistere lo sviluppo della SSRS,
    - riesaminare la SSRS per accertarne la coerenza con le presenti norme di sicurezza e i documenti relativi alla politica e all'architettura INFOSEC,
    - partecipare alle commissioni/comitati di accreditamento ove necessario nonché fornire alla SAA raccomandazioni INFOSEC sull'accreditamento,
    - fornire supporto alle attività di formazione e di informazione INFOSEC,
    - fornire consulenza tecnica nelle indagini sugli incidenti connessi con l'INFOSEC,
    - definire orientamenti tecnici strategici onde garantire che sia utilizzato unicamente software autorizzato.

AUTORITA' OPERATIVA DEL SISTEMA TI (ITSOA)

38. L'autorità INFOSEC delega quanto prima possibile la responsabilità dell'attuazione e della gestione dei controlli e delle caratteristiche specifiche di sicurezza del SISTEMA all'ITSOA. Tale responsabilità permane lungo tutto il ciclo di vita del SISTEMA, a partire dalla fase di concezione del progetto fino alla sua disattivazione finale.

39. L'ITSOA è responsabile di tutte le misure di sicurezza progettate come parte del SISTEMA globale. Le responsabilità includono la preparazione delle SecOP. L'ITSOA specifica le norme e le procedure di sicurezza che il fornitore del SISTEMA è tenuto a rispettare.

40. L'ITSOA può delegare parte delle sue responsabilità, se del caso, per esempio al responsabile della sicurezza INFOSEC e al responsabile della sicurezza del sito INFOSEC. Le varie mansioni INFOSEC possono essere svolte da una sola persona.

UTENTI

41. Tutti gli utenti sono tenuti a garantire che le loro azioni non compromettano la sicurezza del SISTEMA che utilizzano.

FORMAZIONE INFOSEC

42. La formazione e l'informazione INFOSEC è disponibile a vari livelli e per vari membri del personale, a seconda dei casi, dell'SGC, degli organismi decentrati dell'UE o dei dipartimenti dei governi degli Stati membri.

Capitolo IV

Misure di sicurezza non tecniche

SICUREZZA DEL PERSONALE

43. Gli utenti del SISTEMA devono essere in possesso di nulla osta di sicurezza ed avere necessità di sapere, in funzione della classificazione e del contenuto delle informazioni trattate dal loro specifico SISTEMA. L'accesso a determinate attrezzature o a informazioni inerenti alla sicurezza dei SISTEMI richiede uno speciale nulla osta di sicurezza rilasciato in base alle procedure del Consiglio.

44. La SAA designa tutti i posti sensibili e specifica il grado del nulla osta e la sorveglianza necessaria da parte delle persone che li ricoprono.

45. I SISTEMI sono specificati e progettati in modo da facilitare l'attribuzione dei compiti e delle responsabilità al personale onde evitare che una sola persona abbia la conoscenza o il controllo totali dei punti nevralgici per la sicurezza del sistema. Per l'alterazione o la manomissione intenzionale del sistema o della rete sarebbe così necessaria la collusione di due o più persone.

SICUREZZA MATERIALE

46. Le aree TI e le aree di terminali/postazioni remoti (quali definite ai punti 29 e 30) in cui sono trattate informazioni classificate CONFIDENTIEL UE (UE riservatissimo) o di grado superiore con strumenti TI, o in cui è possibile un accesso a tali informazioni, sono classificate come aree di sicurezza di categoria UE I o II o della categoria nazionale equivalente, ove opportuno.

47. Le aree TI e quelle di terminali/postazioni remoti in cui la sicurezza del SISTEMA può essere modificata non sono occupate da un solo funzionario/altro agente abilitato.

CONTROLLO DELL'ACCESSO A UN SISTEMA

48. Tutte le informazioni e il materiale che consentono il controllo dell'accesso a un SISTEMA sono protette da disposizioni commisurate al grado di classificazione e alla designazione di categoria più elevati delle informazioni cui danno accesso.

49. Le informazioni e il materiale per il controllo dell'accesso che non sono più utilizzati a questo scopo vengono distrutte conformemente ai punti da 61 a 63.

Capitolo V

Misure tecniche di sicurezza

SICUREZZA DELLE INFORMAZIONI

50. L'originatore delle informazioni è tenuto a identificare e classificare tutti i documenti contenenti informazioni, siano essi su supporto cartaceo o informatico. Ciascuna pagina delle copie cartacee viene contrassegnata, in testa e in calce, con la pertinente classificazione. I documenti, che siano su supporto cartaceo o informatico, hanno la classificazione più elevata tra quelle attribuite all'informazione utilizzata per produrli. Il modo di funzionamento di un SISTEMA può anche avere un impatto sulla classificazione dei documenti prodotti da tale sistema.

51. Un'organizzazione e coloro che, al suo interno, sono in possesso di informazioni sono tenuti a valutare i problemi inerenti al raggruppamento di singoli elementi informativi, e alle deduzioni che si possono trarre dagli elementi connessi, nonché a determinare se una classificazione di grado più elevato sia pertinente per la totalità delle informazioni così raggruppate.

52. Il fatto che l'informazione possa essere formulata come un codice abbreviato, un codice di trasmissione o qualsiasi altra forma di rappresentazione binaria non conferisce alcuna protezione della sicurezza e non deve, pertanto, incidere sulla classificazione dell'informazione.

53. Quando l'informazione è trasferita da un SISTEMA ad un altro, l'informazione è protetta durante il trasferimento e nel SISTEMA ricevente in modo commisurato alla classificazione e alla categoria originarie dell'informazione.

54. Tutti i mezzi di archiviazione informatica sono trattati in modo commisurato alla classificazione più elevata dell'informazione archiviata o del contrassegno apposto sul mezzo, e opportunamente protetti in ogni momento.

55. I mezzi di archiviazione informatica riutilizzabili usati per registrare informazioni classificate UE mantengono la classificazione più elevata per la quale sono stati usati finché le informazioni in questione non vengono declassate o declassificate e il mezzo di archiviazione riclassificato di conseguenza, oppure il mezzo declassificato o distrutto con una procedura dell'SGC o una procedura nazionale approvata (cfr. punti da 61 a 63).

CONTROLLO E RESPONSABILITA' DELLE INFORMAZIONI

56. I log automatici (audit trail) o manuali sono tenuti quale traccia dell'accesso alle informazioni classificate SECRET EU (UE segreto) o di grado superiore. Queste tracce sono conservate conformemente alle presenti norme di sicurezza.

57. I prodotti classificati UE detenuti nella zona TI possono essere trattati come un elemento classificato e non necessitano di registrazione, purché il materiale sia identificato, contrassegnato con la sua classificazione e controllato in modo appropriato.

58. Allorché un SISTEMA che tratta informazioni classificate UE genera dati che vengono trasmessi da un'area TI all'area di terminali/postazioni remoti, vengono istituite procedure, approvate dalla SAA, per controllare i dati trasmessi. Per le classificazioni di grado SECRET UE (UE segreto) o superiore tali procedure includono specifiche istruzioni per la responsabilità delle informazioni.

TRATTAMENTO E CONTROLLO DEI SUPPORTI INFORMATICI RIMOVIBILI

59. Tutti i supporti informatici rimovibili classificati CONFIDENTIEL UE (UE riservatissimo) o di grado superiore sono trattati come materiale classificato cui si applicano le norme generali. I contrassegni di identificazione e classificazione devono essere adattati alle specifiche caratteristiche fisiche dei supporti, in modo da renderli chiaramente riconoscibili.

60. Spetta agli utenti assicurare che le informazioni classificate UE siano archiviate su supporti provvisti dell'appropriato contrassegno di classificazione e adeguatamente protetti. Sono stabilite procedure atte ad assicurare che, per tutti i gradi di classificazione UE, l'archiviazione delle informazioni su supporti informatici avvenga in conformità delle presenti norme di sicurezza.

DECLASSIFICAZIONE E DISTRUZIONE DI SUPPORTI INFORMATICI

61. I supporti informatici utilizzati per la registrazione di informazioni classificate UE possono essere declassati o declassificati a condizione che siano applicate procedure approvate dall'SGC o nazionali.

62. I supporti informatici che hanno contenuto informazioni TRES SECRET UE/EU TOP SECRET (UE segretissimo) o informazioni di una categoria speciale non sono declassificati né riutilizzati.

63. I supporti informatici che non possono essere declassificati o riutilizzati sono distrutti secondo una procedura approvata dall'SGC o nazionale.

SICUREZZA DELLE COMUNICAZIONI

64. Quando informazioni classificate UE sono trasmesse per via elettromagnetica, si applicano misure speciali atte a proteggere la riservatezza, l'integrità e la disponibilità della trasmissione. La SAA stabilisce i requisiti relativi alla protezione delle trasmissioni dalla detezione e dalle intercettazioni. Le informazioni trasmesse all'interno di un sistema di comunicazioni sono protette tenendo conto dei requisiti di riservatezza, integrità e disponibilità.

65. I metodi crittografici, e i prodotti connessi, che si rendano necessari per la protezione della riservatezza, dell'integrità e della disponibilità sono specificamente approvati a tal fine dalla SAA.

66. Durante la trasmissione la riservatezza delle informazioni classificate SECRET UE (EU segreto) o di grado superiore è protetta mediante metodi o prodotti crittografici approvati dal Consiglio su raccomandazione del Comitato per la sicurezza del Consiglio. Durante la trasmissione la riservatezza delle informazioni classificate CONFIDENTIEL UE (UE riservatissimo) o RESTREINT EU (UE riservato) è protetta mediante metodi o prodotti crittografici approvati dal Segretario generale/Alto rappresentante su raccomandazione del Comitato per la sicurezza del Consiglio o da uno Stato membro.

67. Specifiche istruzioni di sicurezza approvate dal Consiglio su raccomandazione del Comitato per la sicurezza del Consiglio contengono norme particolareggiate applicabili alla trasmissione di informazioni classificate EU.

68. In circostanze operative eccezionali le informazioni classificate RESTREINT EU (UE riservato), CONFIDENTIEL UE (UE riservatissimo) e SECRET EU (UE segreto) possono essere trasmesse sotto forma di testo in chiaro, previa esplicita autorizzazione per ogni singolo caso. Le circostanze eccezionali di cui sopra si verificano:

    a. in situazioni di crisi, conflitti o guerre imminenti o già in corso e

    b. quando la rapidità di consegna è della massima importanza e non sono disponibili strumenti di cifratura, nonché quando si ritiene che le informazioni trasmesse non possano essere sfruttate con rapidità tale da influire negativamente sulle operazioni.

69. Un SISTEMA deve essere in grado di negare con certezza ad una o tutte le sue postazioni o ai suoi terminali remoti l'accesso ad informazioni classificate UE, se necessario disconnettendoli materialmente o mediante speciali caratteristiche del software approvate dalla SAA.

MISURE DI SICUREZZA CONCERNENTI L'INSTALLAZIONE E LE RADIAZIONI

70. Le specifiche relative all'installazione iniziale dei SISTEMI e a qualsiasi successiva modifica di rilievo prevedono che l'installazione sia effettuata da installatori provvisti di nulla osta di sicurezza sotto la costante sorveglianza di personale tecnico qualificato abilitato all'accesso ad informazioni aventi un grado di classificazione UE equivalente al grado più alto delle informazioni che il sistema dovrà archiviare o trattare.

71. Tutte le apparecchiature sono installate conformemente alle vigenti norme di sicurezza del Consiglio.

72. I SISTEMI che trattano informazioni classificate CONFIDENTIEL UE (UE riservatissimo) o di grado superiore sono protetti in modo tale che la loro sicurezza non possa essere minacciata da radiazioni compromettenti, il cui studio e la cui prevenzione sono designati dal termine "TEMPEST".

73. Le contromisure dell'effetto TEMPESTA relative alle installazioni del SGC e degli organismi decentrati dell'UE sono studiate ed approvate da un'autorità TEMPEST designata dall'autorità di sicurezza dell'SGC. L'autorità competente per l'approvazione delle installazioni nazionali che trattano informazioni classificate UE è l'autorità nazionale di approvazione TEMPEST riconosciuta.

Capitolo VI

Sicurezza durante il trattamento

PROCEDURE OPERATIVE DI SICUREZZA

74. Le SecOP definiscono i principi da adottare in materia di sicurezza, le procedure operative da seguire e le responsabilità del personale. Le SecOP sono elaborate sotto la responsabilità dell'ITSOA.

PROTEZIONE DEL SOFTWARE/GESTIONE DELLA CONFIGURAZIONE

75. Il livello di protezione dei programmi applicativi è determinato in base ad una valutazione della classificazione di sicurezza dei programmi stessi piuttosto che delle informazioni che devono trattare. Le versioni dei software in uso devono essere verificate ad intervalli regolari per assicurarne l'integrità ed il corretto funzionamento.

76. Versioni nuove o modificate dei software vengono utilizzate per il trattamento di informazioni classificate UE solo dopo essere state verificate dall'ITSOA.

CONTROLLI CONTRO LA PRESENZA DI SOFTWARE MALIZIOSI/VIRUS INFORMATICI

77. Controlli contro la presenza di software maliziosi/virus informatici sono effettuati periodicamente secondo quanto prescritto dalla SAA.

78. Prima di essere immessi in un SISTEMA, tutti i supporti informatici introdotti nell'SGC o negli organismi decentrati dell'UE ovvero negli Stati membri devono essere controllati al fine di rilevare l'eventuale presenza di software maliziosi o virus informatici.

MANUTENZIONE

79. Nei contratti e nelle procedure concernenti la manutenzione periodica e su richiesta dei SISTEMI per cui sia stata stilata una SSRS sono specificati i requisiti e le disposizioni applicabili al personale addetto alla manutenzione ed alle relative apparecchiature che entrano in una zona TI.

80. Tali requisiti e tali procedure sono chiaramente indicati, rispettivamente, nella SSRS e nelle SecOP. Le operazioni di manutenzione di competenza del contraente che richiedono procedure di telediagnostica sono consentite solo in circostanze eccezionali, sotto rigoroso controllo ed esclusivamente previa approvazione della SAA.

Capitolo VII

Fornitura

81. Qualsiasi prodotto relativo alla sicurezza da utilizzare con il SISTEMA oggetto della fornitura, deve già essere stato valutato e certificato oppure essere in fase di valutazione e certificazione da parte di un apposito organismo, secondo criteri riconosciuti a livello internazionale (quali i criteri comuni per la valutazione della sicurezza delle tecnologie dell'informazione: cfr. ISO 15408)

82. Per decidere se noleggiare piuttosto che acquistare un'attrezzatura, specie supporti informatici, occorre tener presente che, una volta utilizzata per le informazioni classificate UE, tale attrezzatura non potrà essere resa disponibile al di fuori di un ambiente adeguatamente protetto senza prima essere declassificata con il consenso della SAA e che non sempre detto consenso sarà possibile.

ACCREDITAMENTO

83. Tutti i SISTEMI che necessitano in via preventiva, per il trattamento di informazioni classificate UE, di una dichiarazione relativa ai requisiti di sicurezza specifici del sistema, sono accreditati dalla SAA sulla scorta delle informazioni fornite nella suddetta dichiarazione, delle SecOP e di qualsiasi altra documentazione pertinente. I sottosistemi e i terminali/postazioni remoti sono accreditati in quanto parte di tutti i SISTEMI a cui sono collegati. Quando un SISTEMA serve sia il Consiglio che altre organizzazioni, l'SGC e le competenti autorità incaricate della sicurezza approvano l'accreditamento di comune accordo.

84. Il processo di accreditamento può essere espletato secondo un'apposita strategia adeguata ad un determinato SISTEMA, definita dalla SAA.

VALUTAZIONE E CERTIFICAZIONE

85. Prima di essere accreditati, in taluni casi, gli elementi di sicurezza di un SISTEMA nel suo insieme _ hardware, firmware e software _ sono valutati e certificati idonei alla salvaguardia delle informazioni al grado di classificazione desiderato.

86. I requisiti per la valutazione e certificazione sono inclusi nella progettazione del sistema e chiaramente definiti nella SSRS.

87. I processi di valutazione e certificazione sono espletati secondo linee direttrici approvate da personale tecnicamente qualificato e adeguatamente abilitato che opera a nome dell'ITSOA.

88. I gruppi a ciò preposti possono essere inviati da un'autorità nazionale di valutazione o certificazione designata oppure da suoi rappresentanti designati, ad esempio un appaltatore competente e abilitato.

89. I processi di valutazione e certificazione richiesti possono essere di livello inferiore (ed includere, ad esempio, solo gli aspetti dell'integrazione) qualora i SISTEMI siano basati su prodotti per la sicurezza dei computer valutati e certificati in ambito nazionale.

VERIFICA SISTEMATICA DEGLI ELEMENTI DI SICUREZZA PER LA PROROGA DELL'ACCREDITAMENTO

90. L'ITSOA stabilisce procedure di controllo sistematico atte a garantire che tutti gli elementi di sicurezza del SISTEMA siano ancora efficaci.

91. I tipi di cambiamenti che renderebbero necessario un riaccreditamento o che richiedono l'approvazione preventiva della SAA sono chiaramente individuati ed enunciati nella SSRS. Dopo qualsiasi modifica, riparazione o disfunzione che possa avere ripercussioni sugli elementi di sicurezza del SISTEMA, ITSOA provvede a far effettuare una verifica per assicurare il corretto funzionamento dei suddetti elementi. La proroga dell'accreditamento del SISTEMA dipende normalmente da un risultato soddisfacente delle verifiche.

92. Tutti i SISTEMI dotati di elementi di sicurezza sono periodicamente ispezionati o riesaminati dalla SAA. Per i SISTEMI che trattano informazioni classificate EU TRES SECRET/EU TOP SECRET (UE segretissimo) o recanti indicazioni complementari, le ispezioni hanno luogo almeno una volta l'anno.

Capitolo VIII

Utilizzo temporaneo o occasionale

SICUREZZA DEI MICROCOMPUTER/PERSONAL COMPUTER

93. I microcomputer/personal computer (PC) muniti di disco fisso (o altri mezzi di archiviazione permanente), funzionanti sia autonomamente sia in rete, e i dispositivi informatici portatili (quali PC portatili e notebook elettronici) provvisti di disco rigido fisso sono considerati mezzi di archiviazione delle informazioni alla stessa stregua dei dischetti o altri supporti informatici rimovibili.

94. A tali attrezzature è attribuito il livello di protezione, in termini di accesso, gestione, archiviazione e trasporto, corrispondente al più alto grado di classificazione delle informazioni archiviate o elaborate (finché passeranno poi ad un livello di protezione inferiore o subiranno una declassificazione conformemente a procedure approvate).

UTILIZZO DI ATTREZZATURA INFORMATICA PRIVATA PER I LAVORI UFFICIALI DEL CONSIGLIO

95. Per il trattamento delle informazioni classificate UE è vietato utilizzare supporti informatici, software e hardware (quale PC e dispositivi informatici portatili) che siano dotati di memoria, di proprietà privata e rimovibili.

96. Hardware, software e supporti vari di proprietà privata non possono essere introdotti in nessuna zona di categoria I o II dove sono trattate informazioni classificate UE senza il permesso del Capo del servizio di sicurezza dell'SGC, di un Ministero nazionale o del rispettivo organismo decentrato dell'UE.

UTILIZZO DI ATTREZZATURA INFORMATICA APPARTENENTE A UN APPALTATORE O FORNITA DAGLI STATI MEMBRI PER I LAVORI UFFICIALI DEL CONSIGLIO

97. Il Capo del servizio di sicurezza dell'SGC, di un Ministero nazionale o della rispettiva agenzia decentrata dell'UE può permettere l'utilizzo di attrezzatura IT e software detenuti da un appaltatore per i lavori ufficiali del Consiglio. Può essere altresì autorizzato l'utilizzo, da parte di funzionari dell'SGC o di un organismo decentrato dell'UE, di attrezzatura e software forniti dagli Stati membri: in tal caso detta attrezzatura è posta sotto controllo e iscritta nell'apposito inventario dell'SGC. Nell'uno o nell'altro caso, se l'attrezzatura serve al trattamento di informazioni classificate UE, si consulta la SAA competente ai fini di un'adeguata presa in considerazione e applicazione degli elementi INFOSEC applicabili al suo utilizzo.

SEZIONE XII

COMUNICAZIONE DI INFORMAZIONI CLASSIFICATE UE A STATI TERZI O ORGANIZZAZIONI INTERNAZIONALI

PRINCIPI CHE REGOLANO LA COMUNICAZIONE DI INFORMAZIONI CLASSIFICATE UE

1. La comunicazione di informazioni classificate UE a Stati terzi o organizzazioni internazionali è decisa dal Consiglio in base:

   - alla natura e al contenuto delle informazioni stesse,
   - alla necessità di sapere dei destinatari,
   - all'entità dei vantaggi per l'UE.

Allo Stato membro di origine dell'informazione classificata UE è chiesto il consenso alla comunicazione.

2. Siffatte decisioni sono prese caso per caso, a seconda:

   - del livello di cooperazione auspicato con gli Stati terzi o le organizzazioni internazionali interessati,
   - della loro affidabilità - dipendente dal livello di sicurezza che sarebbe attribuito alle informazioni classificate UE affidate a detti Stati o organizzazioni nonché dalla conformità delle norme di sicurezza ivi applicabili a quelle applicate nell'UE; a tale riguardo il Consiglio si avvale del parere tecnico del Comitato per la sicurezza del Consiglio.

3. L'accettazione di informazioni classificate UE da parte di Stati terzi o organizzazioni internazionali implica la garanzia che saranno utilizzate esclusivamente agli scopi per cui sono state comunicate o scambiate e che sarà loro assicurata la protezione richiesta dal Consiglio.

LIVELLI

4. Una volta decisa la comunicazione o lo scambio di informazioni classificate con un determinato Stato o organizzazione internazionale, il Consiglio decide il livello di cooperazione possibile, che dipenderà soprattutto dalla politica seguita in materia di sicurezza e dalla normativa applicata da tale Stato o organizzazione.

5. I livelli di cooperazione sono tre:

   primo livello

   cooperazione con Stati terzi o organizzazioni internazionali la cui politica e normativa in materia di sicurezza sono molto affini a quelle dell'UE;

   secondo livello

   cooperazione con Stati terzi o organizzazioni internazionali la cui politica e normativa in materia di sicurezza sono notevolmente diverse da quelle dell'UE;

   terzo livello

   cooperazione di carattere occasionale con Stati terzi o organizzazioni internazionali di cui non si possono valutare la politica e la normativa in materia di sicurezza.

6. Il livello di cooperazione determina le norme di sicurezza, riformulate nei singoli casi alla luce del parere tecnico del Comitato per la sicurezza del Consiglio, che si chiederà ai beneficiari di applicare alla protezione delle informazioni classificate trasmesse loro. Dette procedure e norme di sicurezza sono descritte dettagliatamente nelle appendici 4, 5 e 6.

ACCORDI

7. Constatata la necessità permanente o a lungo termine di uno scambio di informazioni classificate tra l'UE e Stati terzi o altre organizzazioni internazionali, il Consiglio procede alla stesura di "accordi sulle procedure di sicurezza per lo scambio di informazioni classificate" con essi, dove sono definite le finalità della cooperazione e le disposizioni reciproche sulla protezione delle informazioni scambiate.

8. Nel caso di una cooperazione occasionale di terzo livello, per definizione limitata nel tempo e nelle finalità, un semplice memorandum d'intesa in cui siano definiti la natura delle informazioni classificate da scambiare e gli obblighi reciproci ad esse relativi può sostituirsi agli "accordi sulle procedure di sicurezza per lo scambio di informazioni classificate" purché il grado di classificazione non sia più elevato di RESTREINT UE (UE riservato).

9. Prima di essere presentati al Consiglio per una decisione, i progetti di accordi sulle procedure di sicurezza o di memorandum d'intesa sono approvati dal Comitato per la sicurezza.

10. Le NSA forniscono al Segretario generale/Alto rappresentante tutta l'assistenza necessaria a garantire che le informazioni da divulgare siano utilizzate e protette conformemente ai suddetti accordi o memorandum d'intesa.

Appendice 1

Elenco delle autorità nazionali di sicurezza

BELGIO

Ministère des Affaires Etrangères, du Commerce Extérieur et de la Coopération au Développement
Direction de la sécurité _ A 01
Rue des Petits Carmes, 15
B1000 Bruxelles
Telefono: 322501 85 14
Telefax: 322501 80 58
Telex: 21376
Indirizzo telegrafico: Direction de Sécurité A01 _ MINAFET

DANIMARCA

Politiets Efterretningstjeneste
Borups Alle 266
DK2400 Copenhagen NV
Telefono: 45 33 14 88 88
Telefax: 45 38 19 07 05
Forsvarsministeriet
Forsvarets Efterretningstjeneste
Kastellet 30
DK2100 Copenhagen Ø.
Telefono: 45 33 32 55 66
Telefax: 45 33 93 13 20

GERMANIA

Bundesministerium des Innern
Referat IS 4
AltMoabit 101D
D10559 Berlin
Telefono: 493039 81 15 28
Telefax: 493039 81 16 10

GRECIA

Cemijü Episekeßo EhmijÞy ¢ltmay (CEEHA)
Tpgqerßa Rsqasixsijþm Pkgqouoqiþm (TRP B' JkÜdoy)
Cqaueßo AruÜkeiay
RSC 1020Vokaqcüy (AhÞma)
Ekkada
SgkÝuxma: 00 301655 22 03 (þqey cqaueßot)
00 301655 22 05 (eijorisesqÜxqo)
Uan: 00 301642 69 40
Hellenic National Defence
General Staff (HNDGS)
Intelligence Branch/Security
(INT. BR./SEC.)
STG 1020, Holargos _ Athens
Greece
Telefono: 00 301655 22 03 (office hours)
00 301655 22 05 (24 hours)
Telefax: 00 301642 69 40

SPAGNA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
Carretera Nacional Radial VI, km 8,500
E28023 Madrid
Telefono: 3491372 57 07
Telefax: 3491372 58 08
Email: nsasp@areatec.com

FRANCIA

Secrétariat général de la Défense Nationale
Service de Sécurité de Défense (SGDN/SSD)
51 Boulevard de la TourMaubourg
F75700 Paris 07 SP
Telefono: 330144 18 81 80
Telefax: 330144 18 82 00
Telex: SEGEDEFNAT 200019
Indirizzo telegrafico: SEGEDEFNAT PARIS

IRLANDA

National Security Authority
Department of Foreign Affairs
80 St. Stephens Green
Dublin 2
Telefono: 3531478 08 22
Telefax: 3531478 14 84

ITALIA

Presidenza del Consiglio dei ministri
Autorità nazionale per la sicurezza
Ufficio centrale per la sicurezza
Via della Pineta Sacchetti, 216
I00168 Roma
Telefono: 3906627 47 75
Telefax: 3906614 33 97
Telex: 623876 AQUILA 1
Indirizzo telegrafico: ess: PCMANSUCSIROMA

LUSSEMBURGO

Autorité Nationale de Sécurité
Ministère d'Etat
Boîte Postale 2379
L1023 Luxembourg
Telefono: 352478 22 10 centralino
352478 22 35 diretto
Telefax: 352478 22 43
352478 22 71
Telex: 3481 SERET LU
Indirizzo telegrafico: MIN D'ETAT _ ANS

PAESI BASSI

Ministerie van Binnenlandse Zaken
Postbus 20010
NL2500 EA Den Haag
Telefono: 3170320 44 00
Telefax: 3170320 07 33
Telex: 32166 SYTH NL
Ministerie van Defensie
Militaire Inlichtingendienst (MID)
Postbus 20701
NL2500 ES Den Haag
Telefono: 3170318 70 60
Telefax: 3170318 79 51

AUSTRIA

Bundesministerium für auswärtige Angelegenheiten
Abteilung I.9
Ballhausplatz 2
A1014 Wien
Telefono: 431531 15 34 64
Telefax: 431531 8 52 19

PORTOGALLO

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Avenida Ilha da Madeira, 1
P1449004 Lisboa
Telefono: 35121301 55 10
35121301 00 01, estensione 20 45 37
Telefax: 35121302 03 50

FINLANDIA

Alivaltiosihteeri (Hallinto)/Understatssekreteraren (Administration)
Ulkoasiainministeriö/Utrikesministeriet
Laivastokatu/Maringatan 22
PL/PB 176
FIN00161 Helsinki/Helsingfors
Telefono: 358913 41 53 38
Telefax: 358913 41 53 03

SVEZZA

Utrikesdepartementet
SSSB
S103 39 Stockholm
Telefono: 468405 54 44
Telefax: 468723 11 76

REGNO UNITO

The Secretary (for DIR/5)
PO Box 5656
London EC1A 1 AH
Telefono: 442072 70 87 51
Telefax: 442076 30 14 28
Indirizzo telegrafico: UK Delegation to Security Policy Dept FCO, "marked in Box 5656 for DIR/5".

Appendice 2

Raffronto tra le classificazioni nazionali di sicurezza

Classificazione EU	Très secret UE/EU Top secret	Secret UE	Confidentiel UE	Restreint UE
Classificazione NATO (1)	.	.	.	.
Classificazione WEU	Focal Top Secret	WEU Secret	WEU Confidental	WEU RESTREINT
Belgium	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Denmark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Germany	STRENG GEHEIM	GEHEIM	VS (2) VERTRAULICH	VS NUR FÜR DEN DIENSTGEBRAUCH
Greece	¢jqxy Apüqqgso	Apüqqgso	Elpirsctsijü	PeqioqirlÝmgy vqÞrgy
Spain	Secreto	Reservado	Confidencial	Difusion Limitada
France	Très Secret Défense (3)	Secret Défense	Confidentiel Défense	Diffusion restreinte
Ireland	Top Secret	Secret	Confidential	RESTREINT
Italy	Segretissimo	Segreto	Riservatissimo	Riservato
Luxembourg	Très Secret	Secret	Confidentiel	Diffusion restreinte
Netherlands	STG Zeer Geheim	STG Geheim	STG Confidentieel	-
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Finnland	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Sweden	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
United Kingdom	Top Secret	Secret	Confidential	RESTREINT

(1) NATO: la corrispondenza con i gradi di classificazione della NATO sarà stabilita durante i negoziati per l'accordo di sicurezza tra Unione europea e NATO.

(2) German IA: VS = Verschlusssache.

(3) Francia: : la classificazione —Très Secret Défenseic, relativa alle priorità governative, può essere modificata solo con l'autorizzazione del Primo ministro.

Appendice 3

Guida pratica alla classificazione

La presente guida è uno strumento indicativo, che non può essere interpretato come variante delle disposizioni sostanziali di cui alle sezioni II e III.

Classificazione	quando	chi	contrassegni	Declassamento/declassificazione	/Distruzione
.	.	.	.	chi	quando
TRÈS SECRET UE/EU TOP SECRET (UE segretissimo): Classificazione riservata esclusivamente a informazioni e materiali la cui divulgazione non autorizzata potrebbe arrecare danni di eccezionale gravità agli interessi fondamentali dell'Unione europea o di uno o più Stati membri [SII, punto 1].	La violazione di oggetti contrassegnati TRÈS SECRET UE/EU TOP SECRET (UE segretissimo) avrebbe come probabili conseguenze: – la minaccia diretta della stabilità interna dell'UE, di uno Stato membro o di paesi amici; – danni di eccezionale gravità alle relazioni con governi amici; – la perdita diretta di molte vite umane; – danni di eccezionale gravità all'efficacia operativa o alla sicurezza delle forze degli Stati membri o di altri contributori ovvero all'ininterrotta efficacia di operazioni di sicurezza o intelligence di massima utilità; – un grave danneggiamento, a lungo termine, dell'economia dell'UE o degli Stati membri.	Stati membri: persone debitamente autorizzate (originatori) [SIII, punto 4]; SGC: persone debitamente autorizzate (originatori) [SIII, punto 4], Segretario generale/Alto rappresentante e Segretario generale aggiunto. Gli originatori indicano la data o un termine a partire dal quale le informazioni contenute nel documento potranno essere declassate o declassificate. In caso contrario, essi verificano almeno ogni cinque anni che la classificazione iniziale del documento sia tuttora necessaria.	La classificazione TRÈS SECRET UE/EU TOP SECRET (UE segretissimo) è apposta con mezzi meccanici o a mano sui documenti TRÈS SECRET UE/EU TOP SECRET (UE segretissimo), eventualmente con il contrassegno ESDP relativo alla difesa [SII, punto 8]. Le classificazioni UE sono applicate sulla parte superiore e inferiore di ogni pagina, al centro. Ogni pagina è numerata. Ciascun documento reca un numero di riferimento e una data; il numero di riferimento figura su ciascuna pagina. Qualora i documenti siano distribuiti in più esemplari, ognuno di essi reca un numero di copia che figura sulla prima pagina, a fianco del numero totale di pagine. Tutti gli allegati e il materiale accluso sono elencati sulla prima pagina [SVII, punto 1].	La declassificazione o il declassamento sono di competenza esclusiva dell'originatore, del Segretario generale/Alto rappresentante o del Segretario generale aggiunto, che informano dell'avvenuto cambiamento tutti i successivi destinatari a cui è stato inviato l'originale del documento o una copia [SVIII, punto 9]. I documenti TRÈS SECRET UE/EU TOP SECRET (UE segretissimo) sono distrutti dall'ufficio centrale di registrazione o dalla sottosezione che ne è responsabile. Ogni documento distrutto viene elencato in un certificato di distruzione, firmato dal funzionario di controllo TRÈS SECRET UE/EU TOP SECRET (UE segretissimo) e dal funzionario che assiste alla distruzione il quale deve avere il nulla osta di sicurezza di grado TRÈS SECRET UE/EU TOP SECRET (UE segretissimo). A tal fine nel repertorio viene inserita una nota. L'ufficio di registrazione tiene i certificati di distruzione, unitamente alle schede di distribuzione, per un periodo di dieci anni [SVII, punto 31].	Esemplari in soprannumero e documenti che non servono più devono essere distrutti [SVII, punto 31]. I documenti TRÈS SECRET UE/EU TOP SECRET (UE segretissimo), inclusi quelli classificati e poi scartati nella fase di preparazione, quali copie rovinate, bozze di lavoro, note dattiloscritte e copie su carta carbone, sono distrutti mediante incenerimento, ridotti in pasta, sminuzzati o altrimenti ridotti in forma irriconoscibile e non ricostituibile sotto la supervisione di un funzionario addetto a questo grado di classificazione [SVII, punto 31].

Classificazione	quando	chi	contrassegni	declassamento/declassificazione/distruzione	
				chi	quando
SECRET UE (UE segreto) classificazione riservata esclusivamente a informazioni e a materiali la cui divulgazione non autorizzata potrebbe ledere gravemente gli interessi fondamentali dell'Unione europea o di uno o più Stati membri [SII, punto 2].	La violazione di oggetti contrassegnati SECRET UE (UE segreto) avrebbe come probabili conseguenze: – tensioni internazionali; – un grave pregiudizio alle relazioni con governi amici; – la minaccia diretta della perdita di vite umane o un grave pregiudizio all'ordine pubblico o alla sicurezza o libertà individuale; – danni gravi all'efficacia operativa o alla sicurezza delle forze degli Stati membri o di altri contributori ovvero all'ininterrotta efficacia di operazioni di sicurezza o intelligence di grande utilità; – ingenti danni materiali agli interessi finanziari, monetari, economici e commerciali del l'UE o di uno Stato membro.	Stati membri: persone autorizzate (originatori) [SIII, punto 2]; SGC e organismi decentrati dell'UE: persone autorizzate (originatori) [SIII, punto 2], Direttori generali, Segretario generale/Alto rappresentante e Segretario generale aggiunto. Gli originatori indicano la data o un termine a partire dal quale le informazioni contenute nel documento potranno essere declassate o declassificate. In caso contrario, essi verificano almeno ogni cinque anni che la classificazione iniziale del documento sia tuttora necessaria [SIII, punto 10].	La classificazione SECRET UE (UE segreto) è apposta con mezzi meccanici o a mano sui documenti SECRET UE (UE segreto), eventualmente con il contrassegno ESDP relativo alla difesa [SII, punto 8]. Le classificazioni UE sono applicate sulla parte superiore e inferiore di ogni pagina, al centro. Ogni pagina è numerata. Ciascun documento reca un numero di riferimento e una data; il numero di riferimento figura su ciascuna pagina. Qualora i documenti siano distribuiti in più esemplari, ognuno di essi reca un numero di copia che figura sulla prima pagina, a fianco del numero totale di pagine. Tutti gli allegati e il materiale accluso sono elencati sulla prima pagina [SVII, punto 1].	La declassificazione o il declassamento sono di competenza esclusiva dell'originatore, del Segretario generale/Alto rappresentante o del Segretario generale aggiunto, che informano dell'avvenuto cambiamento tutti i successivi destinatari a cui è stato inviato l'originale del documento o una copia [SVII, punto 9]. I documenti SECRET UE (UE segreto) sono distrutti dall'ufficio di registrazione che ne è responsabile, sotto la sorveglianza di una persona con nulla osta di sicurezza. I documenti SECRET UE (UE segreto) distrutti sono elencati in un certificato di distruzione firmato, detenuto dall'ufficio di registrazione, unitamente alle schede di distribuzione, per almeno tre anni [SVII, punto 32].	Esemplari in soprannumero e documenti che non servono più devono essere distrutti [SVII, punto 31]. I documenti SECRET UE (UE segreto) inclusi quelli classificati e poi scartati nella fase di preparazione quali copie rovinate, bozze di lavoro, note dattiloscritte e copie su carta carbone sono distrutti mediante incenerimento, ridotti in pasta, sminuzzati o altrimenti ridotti in una forma irriconoscibile e non ricostituibile [SVII, punti 31 e 32].

Classificazione	quando	chi	contrassegni	declassamento/declassificazione/distruzione	
				chi	quando
CONFIDENTIEL UE (UE riservatissimo): classificazione riservata a informazioni e materiali la cui divulgazione non autorizzata lederebbe gli interessi fondamentali dell'Unione europea o di uno o più Stati membri [SII, punto 4].	La violazione di oggetti contrassegnati CONFIDENTIEL UE (UE riservatissimo) avrebbe come probabili conseguenze: – un concreto pregiudizio alle relazioni diplomatiche, ad esempio proteste formali o altre sanzioni; – un pregiudizio alla sicurezza o libertà individuale; – danni all'efficacia operativa o alla sicurezza delle forze degli Stati membri o di altri contributori ovvero all'efficacia di importanti operazioni di sicurezza o intelligence; – rischio di compromettere in modo sostanziale la capacità finanziaria delle grandi organizzazioni; – impedimenti alle indagini o agevolazione di reati gravi; – ripercussioni fondamentalmente contrarie agli interessi finanziari, monetari, economici e commerciali dell'UE o degli Stati membri; – gravi impedimenti all'elaborazione o al funzionamento delle grandi politiche dell'UE; – la cessazione o altre gravi perturbazioni delle attività rilevanti dell'UE.	Stati membri: persone autorizzate (originatori) [SIII, punto 2]; SGC e agenzie decentrate dell'UE: persone autorizzate (originatori) [SIII, punto 2,] Direttori generali, Segretario generale/Alto rappresentante e Segretario generale aggiunto. Gli originatori indicano la data o un termine a partire dal quale le informazioni contenute nel documento potranno essere declassate o declassificate. In caso contrario, esso verifica almeno ogni cinque anni che la classificazione iniziale del documento sia tuttora necessaria [SIII, punto 10].	La classificazione CONFIDENTIEL UE (UE riservatissimo) è apposta con mezzi meccanici o a mano sui documenti UE CONFIDENTIEL UE (UE riservatissimo), eventualmente con il contrassegno ESDP relativo alla difesa [SIL, punto 8]. Le classificazioni UE sono applicate sulla parte superiore e inferiore di ogni pagina, al centro. Ogni pagina è numerata. Ciascun documento reca un numero di riferimento e una data. Tutti gli allegati e il materiale accluso sono elencati sulla prima pagina [SVII, punto 1].	La declassificazione e il declassamento sono di competenza esclusiva dell'originatore, del Segretario generale/Alto rappresentante o del Segretario generale aggiunto, che informano dell'avvenuto cambiamento tutti i successivi destinatari a cui è stato inviato l'originale del documento o una copia [SIII, punto 9]. I documenti CONFIDENTIEL UE (UE riservatissimo) sono distrutti dall'ufficio di registrazione che ne è responsabile, sotto la sorveglianza di una persona con nulla osta di sicurezza. La loro distruzione è registrata conformemente alle norme nazionali e, per l'SGC e gli organismi decentrati dell'UE, in base a istruzioni del Segretario generale/Alto rappresentante [SVII, punto 33].	Esemplari in soprannumero e documenti che non servono più devono essere distrutti [SVII, punto 31]. I documenti CONFIDENTIEL UE (UE riservatissimo), inclusi quelli classificati e poi scartati nella fase di preparazione, quali copie rovinate, bozze di lavoro, note dattilografate e copie su carta carbone, sono distrutti mediante incenerimento, o ridotti in pasta, sminuzzati o altrimenti ridotti in una forma irriconoscibile e non ricostituibile [SVII, punti 31c e 33].

Classificazione	quando	chi	contrassegni	declassamento/declassificazione/distruzione	
				chi	quando
RESTREINT UE (UE riservato): classificazione riservata a informazioni e materiali la cui divulgazione non autorizzata potrebbe arrecare danno agli interessi dell'Unione europea o di uno o più Stati membri [SII, punto 4].	La violazione di oggetti contrassegnati RESTREINT UE (UE riservato) avrebbe come probabili conseguenze: – ripercussioni negative sulle relazioni diplomatiche; – notevoli difficoltà per singoli individui; – un più difficile mantenimento dell'efficacia operativa o della sicurezza delle forze degli Stati membri o di altri contributori; – perdite finanziarie o più facili profitti o vantaggi indebiti per singoli individui o società; – il mancato rispetto di regolari impegni al mantenimento della riservatezza di informazioni fornite da terzi; – il mancato rispetto di vincoli regolamentari alla divulgazione di informazioni; – pregiudizio alle indagini o agevolazione di reati; – svantaggi per l'UE o gli Stati membri nei negoziati di carattere commerciale o politico con terzi; – impedimenti a un'efficace elaborazione o funzionamento delle politiche dell'UE; – il rischio di compromettere la buona gestione dell'UE e delle sue attività.	Stati membri: persone autorizzate (originatori) [SIII, punto 2]; SGC e agenzie decentrate dell'UE: persone autorizzate (originatori) [SIII, punto 2], Direttori generali, Segretario generale/Alto rappresentante e Segretario generale aggiunto. Gli originatori indicano la data o un termine a partire dal quale le informazioni contenute nel documento potranno essere declassate o declassificate. In caso contrario, esso verifica almeno ogni cinque anni che la classificazione iniziale del documento sia tuttora necessaria [SIII, punto 10].	La classificazione RESTREINT UE (UE riservato) è apposta con mezzi meccanici o elettronici sui documenti RESTREINT UE (UE riservato), eventualmente con il contrassegno ESDP relativo alla difesa [SII, punto 8]. Le classificazioni UE sono applicate sulla parte superiore e inferiore di ogni pagina, al centro. Ogni pagina è numerata. Ciascun documento reca un numero di riferimento e una data [SVII, punto 1].	La declassificazione e il declassamento sono di competenza esclusiva dell'originatore, del Segretario generale/Alto rappresentante o del Segretario generale aggiunto, che informano dell'avvenuto cambiamento tutti i successivi destinatari a cui è stato inviato l'originale del documento o una copia [SIII, punto 9]. I documenti RESTREINT UE (UE riservato) sono distrutti dall'ufficio di registrazione che ne è responsabile, conformemente alle norme nazionali e, per l'SGC e gli organismi decentrati dell'UE, in base a istruzioni del Segretario generale/Alto rappresentante [SVII, punto 34].	Esemplari in soprannumero e documenti che non servono più devono essere distrutti [SVII, punto 31]

Appendice 4

Linee direttrici per la comunicazione di informazioni classificate UE a stati terzi o organizzazioni internazionali

Cooperazione di primo livello

PROCEDURE

1. La facoltà di decidere la comunicazione di informazioni classificate UE a paesi non firmatari del trattato sull'Unione europea o ad altre organizzazioni internazionali la cui politica in materia di sicurezza e la relativa normativa sono paragonabili a quelle dell'UE spetta al Consiglio.

2. Il Consiglio può delegare la decisione: in tal caso la delega specifica la natura delle informazioni che possono essere comunicate e il loro grado di classificazione, di norma non superiore a CONFIDENTIEL UE (UE RISERVATISSIMO).

3. A condizione che sia stato concluso un accordo in materia di sicurezza, le richieste di comunicazione di informazioni classificate UE sono rivolte al Segretario generale/Alto rappresentante, dagli organismi preposti alla sicurezza degli Stati od organizzazioni internazionali interessati che precisano le finalità nonché la natura delle informazioni classificate richieste.

   Le richieste possono essere altresì presentate da uno Stato membro o da un organismo decentrato dell'UE che ritenga auspicabile la comunicazione di informazioni classificate UE: anch'essi ne dichiarano le finalità e i vantaggi per l'UE, specificando la natura e il grado di classificazione delle informazioni richieste.

4. La richiesta viene esaminata dall'SGC il quale:

   - chiede il parere dello Stato membro o, se del caso, dell'organismo decentrato dell'UE che ha emanato l'informazione richiesta;
   - stabilisce i necessari contatti con gli organismi preposti alla sicurezza degli Stati od organizzazioni internazionali che ne sono i destinatari, per verificare l'idoneità della loro politica e normativa in materia di sicurezza a garantire che le informazioni classificate comunicate siano protette conformemente alle presenti norme di sicurezza;
   - chiede il parere tecnico delle autorità nazionali competenti in materia di sicurezza degli Stati membri in merito alla fiducia che può essere riposta negli Stati o organismi internazionali che ne sono destinatari.

5. L'SGC inoltra la richiesta e la raccomandazione del servizio di sicurezza al Consiglio, affinché prenda una decisione.

NORME DI SICUREZZA CHE DEVONO ESSERE APPLICATE DAI DESTINATARI

6. Il Segretario generale/Alto rappresentante notifica agli Stati od organizzazioni internazionali destinatari la decisione del Consiglio di autorizzare la comunicazione di informazioni classificate UE, inviando le presenti norme di sicurezza in quante copie sono considerate necessarie. In caso di richiesta presentata da uno Stato membro, è quest'ultimo a notificare l'autorizzazione al destinatario.

   La decisione prende effetto soltanto previa garanzia scritta da parte dei destinatari che:

   - l'informazione sarà utilizzata ai soli scopi concordati;
   - la sua protezione sarà conforme alle presenti norme di sicurezza e in particolare alle disposizioni speciali riportate qui di seguito.

7. *Personale*

   a) Il numero di funzionari aventi accesso alle informazioni classificate UE è rigorosamente limitato, secondo il principio della necessità di sapere, alle persone le cui funzioni lo richiedono.

b) Tutti i funzionari o cittadini autorizzati ad accedere alle informazioni classificate CONFIDENTIEL UE (UE RISERVATISSIMO) o di grado superiore sono in possesso di un attestato per un determinato grado di protezione o dell'equivalente nulla osta di sicurezza l'uno e l'altro emessi dal proprio governo nazionale.

8. *Trasmissione di documenti*

a) Le procedure pratiche per la trasmissione di documenti sono concordate in base alle disposizioni della sezione VII delle norme di sicurezza del Consiglio e forniscono indicazioni precise soprattutto sulle sezioni dell'Ufficio di registrazione a cui devono essere inoltrate le informazioni classificate UE.

b) Se l'autorizzazione del Consiglio riguarda la comunicazione di informazioni classificate anche di grado TRES SECRET UE/EU TOP SECRET (UE SEGRETISSIMO), lo Stato o l'organizzazione internazionale che ne sono destinatari istituiscono un ufficio centrale di registrazione UE, eventualmente suddiviso in sezioni. Ad essi si applicano le disposizioni della sezione VIII delle presenti norme di sicurezza.

9. Registrazione

Non appena riceve un documento classificato UE CONFIDENTIEL (UE RISERVATISSIMO) o di grado superiore, l'ufficio di registrazione lo annota in un registro speciale dell'organizzazione, suddiviso in colonne per la data di ricezione, dettagli del documento (data, numero di riferimento e di copia), la classificazione, il titolo, il nome o la qualifica del ricevente, la data di ritorno della ricevuta e la data di rinvio del documento all'originatore UE o dell'avvenuta distruzione.

10. *Distruzione*

a) I documenti classificati UE vengono distrutti secondo le istruzioni riportate nella sezione VI delle presenti norme di sicurezza: l'avvenuta distruzione di documenti classificati SECRET UE (UE SEGRETO) e TRES SECRET UE/EU TOP SECRET (UE SEGRETISSIMO) è attestata con certificati inviati in copia all'ufficio di registrazione UE che li aveva trasmessi.

b) I documenti classificati UE sono inclusi nei programmi di distruzione d'emergenza predisposti per i documenti classificati degli organismi destinatari.

11. Protezione *dei documenti*

Non sarà tralasciata alcuna misura che possa impedire l'accesso di persone non autorizzate alle informazioni classificate UE.

12. *Copie, traduzioni ed* estratti

E' vietato fotocopiare o tradurre un documento classificato CONFIDENTIEL UE (UE RISERVATISSIMO) o SECRET UE (UE SEGRETO), oppure estrarne brani senza l'autorizzazione del responsabile della sicurezza, che registrerà e controllerà copie, traduzioni o estratti apponendovi, se necessario, una stampigliatura.

La riproduzione o traduzione di un documento classificato TRES SECRET UE/EU TOP SECRET (UE SEGRETISSIMO) può essere autorizzata soltanto dall'autorità d'origine, che preciserà il numero di copie autorizzate; se non è possibile risalire a tale autorità, la richiesta è deferita al servizio di sicurezza dell'SGC.

13. *Violazione delle norme di sicurezza*

In caso di violazione, presunta o reale, delle norme di sicurezza per un documento classificato UE, si dovrebbe immediatamente procedere, fatta salva la conclusione di un accordo in materia di sicurezza, a:

a) effettuare un'indagine per accertare le circostanze di detta violazione;

b) informare il servizio di sicurezza dell'SGC, l'autorità nazionale competente in materia di sicurezza e l'autorità d'origine o dichiarare chiaramente, se del caso, che quest'ultima non è stata informata;

c) prendere misure concrete per limitare al minimo gli effetti della violazione;

d) riesaminare e applicare le misure atte ad impedire nuovi episodi;

e) porre in atto tutte le misure raccomandate dal servizio di sicurezza dell'SGC per impedire nuovi episodi.

14. *Ispezioni*

Il servizio di sicurezza dell'SGC sarà autorizzato, con il consenso degli Stati od organizzazioni internazionali interessati, ad effettuare una valutazione dell'efficacia delle misure prese a protezione delle informazioni classificate UE che sono state comunicate a terzi.

15. *Relazioni*

Fatta salva la conclusione di accordi in materia di sicurezza, gli Stati o le organizzazioni internazionali dovrebbero, fintanto che detengono informazioni classificate UE, presentare una relazione annuale a conferma del rispetto delle presenti norme di sicurezza, entro una data specificata al momento in cui è stata autorizzata la comunicazione dell'informazione.

Appendice 5

Linee direttrici per la comunicazione d'informazioni classificate UE a stati terzi o organizzazioni internazionali

Cooperazione di secondo livello

PROCEDURE

1. La facoltà di comunicare informazioni classificate UE a Stati terzi o organizzazioni internazionali la cui politica e normativa di sicurezza sono molto diverse da quelle dell'UE spetta al Consiglio. In linea di principio, è limitata alle informazioni classificate fino al grado SECRET UE (UE SEGRETO) compreso; ne sono escluse le informazioni nazionali che sono di competenza specifica degli Stati membri e le categorie di informazioni classificate UE protette da speciali contrassegni.

2. Il Consiglio può delegare la decisione: nel delegarla, entro i limiti definiti nel paragrafo 1, specifica la natura delle informazioni che possono essere comunicate e il loro grado di classificazione, che non è superiore a RESTREINT UE (UE RISERVATO).

3. A condizione che sia stato concluso un accordo in materia di sicurezza, le richieste di comunicazione di informazioni classificate UE sono rivolte al Segretario generale/Alto rappresentante dagli organismi preposti alla sicurezza degli Stati o organizzazioni internazionali interessati, che precisano le finalità nonché la natura e il grado di classificazione delle informazioni richieste.

   Le richieste possono essere altresì presentate da uno Stato membro o da un organismo decentrato dell'UE che ritenga auspicabile la comunicazione di informazioni classificate UE: anch'essi ne dichiarano le finalità e i vantaggi per l'UE, specificando la natura e il grado di classificazione delle informazioni richieste.

4. La richiesta viene esaminata dall'SGC il quale

   – chiede il parere dello Stato membro o, se del caso, dell'organismo decentrato UE che ha emanato le informazioni da comunicare;

   – prende i primi contatti con gli organismi preposti alla sicurezza degli Stati o organizzazioni internazionali destinatari per avere informazioni sulla loro politica e la loro normativa in fatto di sicurezza e in particolare per compilare una tabella in cui sono messe a confronto le classificazioni applicate nell'UE e quelle dello Stato o dell'organizzazione interessata;

   – organizza una riunione del Comitato per la sicurezza del Consiglio o, se necessario con la procedura di approvazione tacita, indaga presso le autorità degli Stati membri per ottenere il parere tecnico del Comitato per la sicurezza.

5. Il parere tecnico del Comitato per la sicurezza del Consiglio verte su quanto segue:

   – la fiducia che si può riporre negli Stati o organizzazioni internazionali destinatari allo scopo di valutare i rischi di sicurezza che corrono l'UE o gli Stati membri;

   – una valutazione della capacità dei destinatari di proteggere le informazioni classificate e comunicate dall'UE;

   – proposte circa le procedure pratiche per il trattamento delle informazioni classificate UE (fornendo versioni parziali di un testo, per esempio) e dei documenti trasmessi (mantenendo o cancellando le diciture di classificazione UE, contrassegni specifici ecc.) [1];

   – il declassamento o la declassificazione da parte dell'autorità d'origine prima che le informazioni siano comunicate agli Stati o organizzazioni internazionali destinatari.

---

[1] Ciò comporta che l'autorità d'origine applichi la procedura definita nel paragrafo 9, sezione III, a tutte le copie diffuse all'interno dell'UE.

6. Il Segretario generale/Alto rappresentante invia al Consiglio, per ottenerne una decisione, la richiesta e il parere tecnico del Comitato per la sicurezza del Consiglio, ottenuto dal Servizio di sicurezza dell'SGC.

NORME DI SICUREZZA CHE I DESTINATARI DEVONO APPLICARE

7. Il Segretario generale/Alto rappresentante porta a conoscenza degli Stati o organizzazioni internazionali destinatari la decisione del Consiglio di autorizzare la comunicazione di informazioni classificate insieme con una tabella in cui sono comparate le classificazioni applicate all'interno dell'UE e quelle degli Stati o organizzazioni interessati. In caso di richiesta presentata da uno Stato membro, è quest'ultimo a notificare l'autorizzazione al destinatario.

   La decisione prende effetto soltanto previa garanzia scritta da parte dei destinatari che:

   - l'informazione sarà utilizzata ai soli scopi concordati;
   - la sua protezione sarà conforme alle norme stabilite dal Consiglio.

8. Vengono fissate le norme di protezione sotto esposte a meno che il Consiglio, ottenuto il parere tecnico del Comitato per la sicurezza del Consiglio, decida di adottare una particolare procedura per il trattamento dei documenti classificati UE (cancellando la menzione della classificazione UE, contrassegni specifici ecc.). In tal caso le norme sono adattate.

9. *Personale*

   a) Il numero dei funzionari aventi accesso alle informazioni classificate UE è rigorosamente ristretto, secondo il principio della necessità di sapere, alle persone le cui funzioni lo richiedono.

   b) Tutti i funzionari o i cittadini autorizzati ad accedere alle informazioni classificate comunicate dall'UE devono avere un nulla osta di sicurezza o un'autorizzazione nazionale per accedere, nel caso di informazioni classificate nazionali, a un determinato livello equivalente a quello dell'UE, secondo la definizione della tabella comparativa.

   c) I nulla osta di sicurezza o autorizzazioni nazionali sono inviati per informazione al Segretario generale/Alto rappresentante.

10. *Trasmissione di documenti*

   a) Le procedure pratiche per la trasmissione di documenti sono concordate tra il Servizio di sicurezza dell'SGC e gli organismi preposti alla sicurezza degli Stati o organizzazioni internazionali destinatari in base alle norme stabilite nella sezione VII delle presenti norme. Vi sono specificati in particolare gli indirizzi esatti ai quali i documenti devono essere inoltrati nonché il corriere o i servizi postali usati per la trasmissione delle informazioni classificate UE.

   b) I documenti classificati CONFIDENTIEL UE (UE RISERVATISSIMO) e gradi superiori sono trasmessi in doppia busta. La busta interna è contrassegnata "UE" e reca la classificazione di sicurezza. A ciascun documento classificato è acclusa una ricevuta. La ricevuta, di per sé non classificata, cita soltanto i dettagli del documento (sigla, data, numero di esemplari) e la lingua, ma non il titolo.

   c) La busta interna è posta in un'altra busta che reca il numero del plico per scopi di ricevimento. La busta esterna non reca alcuna classificazione di sicurezza.

   d) Ai corrieri è sempre fornita una ricevuta con il numero del plico.

11. *Registrazione al* momento *dell'arrivo*

   La NSA dello Stato destinatario o il suo equivalente, che riceve le informazioni classificate inviate dall'UE a nome del proprio governo, ovvero l'ufficio di sicurezza dell'organizzazione internazionale destinataria, istituisce uno speciale registro per annotare le informazioni classificate UE all'atto del ricevimento. Il registro contiene colonne con l'indicazione della data, dettagli del documento (data, sigla e numero di esemplari), classificazione, titolo, nome o titolo del destinatario, data del ritorno della ricevuta e la data del rinvio del documento all'UE o quella della distruzione del documento.

12. *Rinvio* dei *documenti*

Il destinatario che rinvia un documento classificato al Consiglio o allo Stato membro che glielo ha inviato, procede come indicato al paragrafo 10.

13. *Protezione*

a) I documenti che non sono in uso, sono custoditi in un contenitore di sicurezza omologato per la custodia di materiali dello stesso grado di classificazione, classificati a livello nazionale. Il contenitore non reca indicazioni del contenuto, è accessibile soltanto a persone autorizzate a trattare informazioni classificate UE. Per quanto riguarda le serrature a combinazione, questa è nota soltanto ai funzionari dello Stato o dell'organizzazione che sono autorizzati ad accedere alle informazioni classificate UE custodite nel contenitore ed è sostituita ogni sei mesi o quando un funzionario viene trasferito, oppure se a uno dei funzionari che conoscono la combinazione viene ritirato il nulla osta di sicurezza o se vi è un rischio di violazione.

b) I documenti classificati UE sono tolti dal contenitore di sicurezza solo dai funzionari che hanno ricevuto il nulla osta per l'accesso ai documenti classificati UE e hanno necessità di sapere. Essi sono responsabili della custodia sicura dei documenti finché ne sono in possesso e in particolare garantiscono che nessuna persona non autorizzata abbia accesso ai documenti. Assicurano anche che i documenti siano custoditi in un contenitore di sicurezza quando hanno finito di consultarli e al di fuori dell'orario di lavoro.

c) Non è permesso fare fotocopie di un documento classificato CONFIDENTIEL UE (UE RISERVATISSIMO) o di grado superiore né trarne estratti senza l'autorizzazione del Servizio di sicurezza dell'SGC.

d) E' necessario che la procedura per una rapida e totale distruzione dei documenti in caso di emergenza sia definita e confermata in collaborazione con il Servizio di sicurezza dell'SGC.

14. *Sicurezza materiale*

a) Quando non sono usati, i contenitori di sicurezza adibiti alla custodia dei documenti classificati UE devono essere chiusi a chiave in permanenza.

b) Il personale addetto alla manutenzione o alle pulizie che deve entrare o lavorare in una stanza in cui sono situati i contenitori di sicurezza deve essere scortato continuamente da un membro del servizio di sicurezza dello Stato o dell'organizzazione o dal funzionario che è direttamente responsabile per la supervisione della sicurezza della stanza stessa.

c) Al di fuori dell'orario di lavoro normale (la notte, nei fine settimana e nei giorni festivi) i contenitori di sicurezza che custodiscono documenti classificati UE sono protetti da una guardia o da un sistema d'allarme automatico.

15. *Violazioni della sicurezza*

Se si è verificata o si sospetta che si sia verificata una violazione della sicurezza relativamente a un documento classificato UE occorre immediatamente provvedere a:

a) inviare subito una relazione al Servizio di sicurezza dell'SGC o alla NSA dello Stato membro che ha preso l'iniziativa di inviare documenti (con copia al Servizio di sicurezza dell'SGC);

b) condurre un'inchiesta al termine della quale è presentata al servizio di sicurezza una relazione completa. Sono poi adottate le misure necessarie per porre rimedio alla situazione.

16. *Ispezioni*

Il Servizio di sicurezza dell'SGC può, con l'accordo degli Stati o organizzazioni internazionali interessati, valutare l'efficacia delle misure per la protezione delle informazioni classificate UE che sono state comunicate.

17. *Relazioni*

Gli Stati o le organizzazioni presentano, fintanto che detengono informazioni classificate UE, una relazione annuale a conferma del rispetto delle presenti norme di sicurezza, entro una data specificata al momento in cui è stata autorizzata la comunicazione dell'informazione.

Appendice 6

Linee direttrici per la comunicazione di informazioni classificate UE a Stati terzi o organizzazioni internazionali

Cooperazione di terzo livello

PROCEDURE

1. Di quando in quando, in circostanze particolari, è possibile che il Consiglio intenda cooperare con Stati o organizzazioni che non possono dare le garanzie richieste dalle presenti norme di sicurezza ma che tale cooperazione richieda la comunicazione di informazioni classificate UE. Le informazioni comunicate non comprendono informazioni nazionali, specificamente riservate agli Stati membri.

2. In tali circostanze particolari, le richieste di cooperazione con l'UE da parte di Stati terzi o di organizzazioni internazionali, ovvero proposte dagli Stati membri o, eventualmente, da organismi decentrati UE, sono esaminate sotto il profilo dei contenuti dal Consiglio, il quale, se è necessario, chiede il parere dello Stato membro o dell'organismo decentrato che è all'origine delle informazioni. Il Consiglio valuta se comunicare le informazioni classificate, considera la necessità di sapere dei destinatari e decide quali informazioni classificate possano essere comunicate.

3. Se il Consiglio è favorevole, spetta al Segretario generale/Alto rappresentante convocare il Comitato per la sicurezza del Consiglio o contattare le autorità di sicurezza nazionali degli Stati membri, eventualmente con la procedura di approvazione tacita, per ottenere il parere tecnico del Comitato per la sicurezza.

4. Il parere tecnico del Comitato per la sicurezza del Consiglio verte:

   a) su una valutazione dei rischi di sicurezza corsi dall'UE o dagli Stati membri;

   b) sulla classificazione delle informazioni che possono essere comunicate, eventualmente in base alla loro natura;

   c) sul declassamento o sulla declassificazione delle informazioni da parte dell'autorità d'origine prima che esse siano comunicate ai paesi o alle organizzazioni internazionali interessati [(1)];

   d) sulle procedure per il trattamento dei documenti da divulgare (vedi paragrafo 5 infra);

   e) sui metodi di trasmissione (servizi postali, sistemi di telecomunicazioni pubblici o protetti, valigia diplomatica, corrieri autorizzati, ecc.).

5. I documenti comunicati a Stati o organizzazioni che rientrano in questa appendice sono predisposti, in linea di massima, senza un riferimento alla fonte o a una classificazione UE. Il Comitato per la sicurezza del Consiglio può raccomandare:

   – l'uso di un contrassegno o codice specifico:

   – l'uso di un sistema di classificazione specifico che rapporta la sensibilità delle informazioni alle necessarie misure di controllo dei metodi usati dal destinatario per trasmettere i documenti (vedi esempi nel paragrafo 14).

6. Il Servizio di sicurezza dell'SGC sottopone al Consiglio il parere tecnico del Comitato per la sicurezza aggiungendo, se necessario, le proposte deleghe di potere necessarie nella fattispecie, in particolare in caso di urgenza.

7. Dopo che il Consiglio ha approvato la comunicazione di informazioni classificate UE e le procedure pratiche di attuazione, il Servizio di sicurezza dell'SGC stabilisce i necessari contatti con l'organismo preposto alla sicurezza dello Stato o organizzazione interessati per facilitare l'applicazione delle misure di sicurezza prospettate.

---

(1) Ciò comporta che l'autorità d'origine applichi la procedura definita al paragrafo 9, sezione III, a tutte le copie diffuse all'interno del UE.

8. Il Servizio di sicurezza dell'SGC distribuisce una tabella di riferimento a tutti gli Stati membri e eventualmente agli organismi decentrati UE interessati nella quale è sintetizzata la natura e la classificazione delle informazioni e sono elencate le organizzazioni e gli Stati ai quali queste possono essere comunicate, secondo quanto deciso dal Consiglio.

9. La NSA nazionale preposta alla sicurezza dello Stato membro all'origine della comunicazione o il Servizio di sicurezza dell'SGC prendono le misure necessarie per facilitare la valutazione di qualsiasi possibile danno e la revisione delle procedure.

10. Si torna a far riferimento al Consiglio tutte le volte che le condizioni di cooperazione subiscono un cambiamento.

NORME DI SICUREZZA CHE DEVONO ESSERE APPLICATE DAI DESTINATARI

11. Il Segretario generale/Alto rappresentante porta a conoscenza degli Stati o delle organizzazioni internazionali destinatari la decisione del Consiglio di autorizzare la comunicazione di informazioni classificate UE, insieme con le norme di protezione dettagliate proposte dal Comitato per la sicurezza del Consiglio e approvata dal Consiglio stesso. Se la richiesta è stata fatta da uno Stato membro, questo lo notifica al destinatario della comunicazione autorizzata.

    La decisione entra in vigore soltanto quando i destinatari danno assicurazione scritta:

    - di non destinare le informazioni ad un uso che non sia la cooperazione decisa dal Consiglio;
    - di dare alle informazioni la protezione richiesta dal Consiglio.

12. *Trasmissione di documenti*

    a) Le procedure pratiche per la trasmissione di documenti sono concordate tra il Servizio sicurezza dell'SGC e gli organi preposti alla sicurezza degli Stati e organizzazioni internazionali destinatari. Sono specificati in particolare gli indirizzi esatti ai quali i documenti devono essere inviati.

    b) I documenti classificati CONFIDENTIEL UE (UE RISERVATISSIMO) e gradi superiori sono trasmessi in doppia busta. La busta interna reca lo specifico timbro o codice convenuto e la menzione della classificazione particolare che è stata approvata per il documento. Per ciascun documento classificato è acclusa una ricevuta. La ricevuta, di per sé non classificata, cita soltanto i dettagli del documento (sigla, data, numero di esemplari) e la lingua, ma non il titolo.

    c) La busta interna è posta in un'altra busta che reca il numero del plico per scopi di ricevimento. La busta esterna non reca alcuna classificazione di sicurezza.

    d) Ai corrieri è sempre fornita una ricevuta con il numero del plico.

13. *Registrazione al momento dell'arrivo*

    La NSA nazionale preposta alla sicurezza dello Stato destinatario o il suo equivalente, che riceve le informazioni classificate inviate dall'UE a nome del proprio governo, ovvero l'ufficio di sicurezza dell'organizzazione internazionale destinataria, istituisce uno speciale registro per annotare le informazioni classificate UE all'atto del ricevimento.

    Il registro contiene colonne con l'indicazione della data, dettagli del documento (data, sigla e numero di esemplari), classificazione, titolo, nome o titolo del destinatario, data del ritorno della ricevuta e la data del rinvio del documento all'UE o quella della distruzione del documento.

14. *Utilizzazione e* protezione *delle informazioni classificate scambiate*

    a) Le informazioni a livello SECRET UE (UE SEGRETO) sono trattate da funzionari specificamente designati che sono autorizzati ad avere accesso alle informazioni con questa classificazione. Sono custodite in armadi di sicurezza di buona qualità che possono essere aperti soltanto da persone autorizzate ad avere accesso alle informazioni che contengono. I luoghi in cui detti armadi sono situati sono sorvegliati costantemente; un sistema di verifica garantisce che possono entrarvi soltanto le persone debitamente autorizzate. Le informazioni di livello SECRET UE (UE SEGRETO) sono inviate per valigia diplomatica, servizi postali e servizi di telecomunicazioni protetti. Un documento SECRET UE (UE SEGRETO) può essere copiato soltanto con l'accordo scritto dell'autorità d'origine. Tutte le copie sono registrate e controllate. Per tutte le operazioni relative a documenti SECRET UE (UE SEGRETO) sono rilasciate ricevute.

b) Le informazioni di livello CONFIDENTIEL UE (UE RISERVATISSIMO) sono trattate da funzionari debitamente designati autorizzati a conoscere l'argomento. I documenti sono custoditi in armadi di sicurezza chiusi a chiave in luoghi controllati.

Le informazioni di livello CONFIDENTIEL UE (UE RISERVATISSIMO) sono inviate per valigia diplomatica, servizi postali militari e telecomunicazioni protette. L'organismo ricevente può farne delle copie, il relativo numero e la distribuzione sono annotati in speciali registri.

c) Le informazioni di livello RESTREINT UE (UE RISERVATO) sono trattate in luoghi non accessibili a personale non autorizzato e custodite in contenitori chiusi a chiave. I documenti possono essere inviati tramite i servizi postali pubblici come plico raccomandato in doppia busta; in casi di emergenza durante le operazioni, tramite sistemi di telecomunicazioni pubblici non protetti. I destinatari possono copiarli.

d) Le informazioni non classificate non richiedono speciali misure di protezione e possono essere inviate per posta e tramite i sistemi pubblici di telecomunicazioni. I destinatari possono copiarle.

15. *Distruzione*

I documenti che non servono più devono essere distrutti. Nel caso di documenti del livello EU RESTREINT UE (UE RISERVATO) e CONFIDENTIEL UE (UE RISERVATISSIMO), viene inserita una nota in un registro speciale. Nel caso di documenti del livello SECRET UE (UE SEGRETO), sono rilasciati certificati di distruzione firmati da due testimoni della distruzione.

16. *Violazioni della sicurezza*

Se informazioni di livello CONFIDENTIEL UE (UE RISERVATISSIMO) o SECRET UE (UE SEGRETO) sono compromesse o se vi è un sospetto in tal senso, la NSA dello Stato o il capo del servizio di sicurezza dell'organizzazione conduce un'inchiesta per appurare le circostanze della violazione. Se i risultati dell'inchiesta sono positivi, questi sono notificati all'autorità di origine. Si provvede a rimediare alle procedure o ai metodi di custodia inadeguati che possano essere all'origine della violazione. Il Segretario generale/Alto rappresentante del Consiglio o la NSA dello Stato membro che ha comunicato le informazioni compromesse può chiedere al destinatario dettagli dell'indagine.

ALLEGATO 2

AGGIORNAMENTO DELL'ORGANIZZAZIONE NAZIONALE PER LA SICUREZZA AI FINI DELLA TUTELA DELLE INFORMAZIONI UE CLASSIFICATE

SOMMARIO

PARTE I

AMBITO DI APPLICAZIONE E DEFINIZIONI

AMBITO DI APPLICAZIONE

1. Le norme, di rilevanza interna, contenute nella alla *Decisione 2001/264/CE del Consiglio dell'Unione europea del 19 marzo 2001, che adotta le norme di sicurezza del Consiglio*, si applicano alla pubblica amministrazione e ogni altra persona giuridica, ente, associazione od organismo che, per fini istituzionali o contrattuali, hanno necessità di conoscere, trattare e custodire informazioni, documenti e materiali UE classificati.

DEFINIZIONI

2. Si intende per:

a) "*Organizzazione nazionale per la sicurezza* ", il complesso degli uffici e di qualunque unità amministrativa, organizzativa, produttiva o di servizio, della pubblica amministrazione e di ogni altra persona giuridica, ente, associazione od organismo, legittimati alla conoscenza, trattazione e gestione delle informazioni, dei documenti e dei materiali classificati, finalizzato ad assicurare modalità di gestione uniformi e sicure e protezione ininterrotta alle informazioni, ai documenti e ai materiali classificati;

b) "*Autorità nazionale per la sicurezza*" – in seguito ANS - il Presidente del Consiglio dei ministri ovvero l'Organo dallo stesso delegato per l'esercizio dei compiti e delle funzioni in materia di tutela delle informazioni, dei documenti e dei materiali classificati;

c) "*Ufficio centrale per la sicurezza*" –in seguito UCSI – l'Ufficio della segreteria Generale del Comitato esecutivo per i servizi di informazione e di sicurezza (CESIS) di cui l'ANS si avvale direttamente per l'esercizio dei compiti e delle funzioni in materia di tutela delle informazioni, dei documenti e dei materiali classificati;

d) "*Ufficio centrale di registrazione UE-SEGRETISSIMO*" – in seguito *ufficio centrale di registrazione* – l'unità amministrativa, istituita presso l'ANS-UCSI, responsabile della ricezione e trasmissione, dall'estero e per l'estero, dei documenti e materiali UE-SEGRETISSIMO, nonché della distribuzione e controllo, nel territorio nazionale, dei medesimi;

e) "*Organo centrale di sicurezza*", l'organo di vertice istituito presso ciascun ministero, Forza armata e qualunque altro ente, associazione od organismo a cui la legge, il regolamento o altre disposizioni amministrative attribuiscono la responsabilità di direzione, coordinamento e controllo, nei confronti dell'intera organizzazione di sicurezza tecnicamente dipendente, in materia di sicurezza e tutela delle informazioni, dei documenti e dei materiali classificati, sotto qualunque forma espressi e gestiti;

f) "*Organo di sicurezza UE*", l'unità amministrativa: Segreteria Speciale UE/SS, Segreteria UE/S, Punto di Controllo UE/SS o Punto di Controllo UE/S, preposta alla tutela delle informazioni, dei documenti e dei materiali UE classificati;

g) "*Funzionario o ufficiale alla sicurezza*", il dirigente, funzionario o ufficiale al quale la massima autorità dell'ente o comando di appartenenza attribuisce la responsabilità di coordinamento e controllo di tutte le attività che concernono la tutela delle informazioni, dei documenti e dei materiali UE classificati;

h) "*Funzionario o ufficiale COMSEC*", il dirigente, funzionario o ufficiale al quale la massima autorità dell'ente o comando o, in via eccezionale, il funzionario o ufficiale alla sicurezza e, per ogni altra persona giuridica, ente, associazione od organismo, il rappresentante legale, attribuisce la responsabilità della corretta applicazione delle norme COMSEC relative alla tutela delle informazioni UE classificate;

i) "*Custode del materiale crittografico*", il responsabile della trattazione e della custodia del materiale COMSEC e crittografico per la tutela delle informazioni UE classificate;

l) "*Incaricato alla sicurezza EAD*", il responsabile del coordinamento, dell'integrazione e della corretta applicazione di tutti gli aspetti della sicurezza fisica, personale, delle informazioni, delle procedure e tecnica dei sistemi EAD dell'ente, comando e ogni altra persona giuridica, ente, associazione od organismo, concernenti la protezione e la tutela delle informazioni UE classificate;

m) "*Gestione delle informazioni UE classificate*", l'originazione, la ricezione, la registrazione, la trattazione, la riproduzione, la preparazione dei plichi, la spedizione, la contabilizzazione, la diramazione, la conservazione, la custodia, l'archiviazione, il trasporto, la distruzione autorizzata e la protezione fisica e logica delle informazioni, dei documenti e dei materiali UE classificati;

n) "*Qualifica UE*", la sigla UE che, premessa ad un'informazione, documento o materiale dell'Unione europea recante un livello o grado di segretezza, determina che quell'informazione concerne la sicurezza dell'Unione europea e degli Stati membri e dev'essere gestita in conformità alle disposizioni contenute nella *Decisione* del Consiglio dell'Ue del 19 marzo 2001 ed alle altre disposizioni emanate dall'ANS;

o) "*Nulla osta di sicurezza*" – in seguito NOS – l'abilitazione di sicurezza necessaria per l'accesso delle persone fisiche alla conoscenza delle informazioni, dei documenti e dei materiali UE classificati, a seconda del livello o grado concesso, RISERVATISSIMO, SEGRETO e SEGRETISSIMO.

PARTE II

ORGANIZZAZIONE NAZIONALE PER LA SICUREZZA

ARTICOLAZIONE DELL'ORGANIZZAZIONE NAZIONALE PER LA SICUREZZA.

3. L'organizzazione nazionale per la sicurezza si articola in:

a) Autorità nazionale per la sicurezza;

b) Ufficio centrale per la sicurezza;

c) organi centrali di sicurezza;

d) organi di sicurezza.

AUTORITÀ NAZIONALE PER LA SICUREZZA.

4. L'Autorità nazionale per la sicurezza esercita le funzioni concernenti la tutela di tutte le informazioni, documenti e materiali classificati, inclusi quelli qualificati UE, e sovrintende a tutte le attività ad esse relative.
Per quanto concerne le informazioni UE classificate l'ANS è responsabile, in particolare, per:

a) il mantenimento della sicurezza delle informazioni UE classificate custodite da qualunque soggetto sottoposto alla giurisdizione italiana, sia esso pubblico o privato, in Italia o all'estero;

b) autorizzare il funzionario di controllo dell'*ufficio centrale di registrazione,* istituito presso l'Ufficio centrale per la sicurezza, per la costituzione e assegnazione dei registri UE-SEGRETISSIMO;

c) l'ispezione periodica, diretta o delegata, agli organi centrali e periferici di sicurezza, in Italia e all'estero, finalizzate a verificare l'idoneità dei dispositivi di sicurezza per la protezione dei siti dove sono conservate e gestite informazioni UE classificate, nonché l'esatta applicazione delle procedure inerenti alla gestione delle medesime;

d) garantire che tutti i cittadini italiani e gli stranieri, impiegati presso enti pubblici e privati nazionali in Italia e all'estero, prima di avere accesso ad informazioni classificate UE-SEGRETISSIMO, UE-SEGRETO e UE-RISERVATISSIMO siano stati debitamente abilitati mediante il rilascio di appropriato nulla osta di sicurezza;

e) verificare che presso tutti gli enti pubblici e privati autorizzati alla gestione di informazioni UE classificate sia stato emanato il regolamento interno di sicurezza (RIS) per la tutela delle informazioni UE classificate - o aggiornato quello esistente - nonché i piani di sicurezza finalizzati ad evitare che, in casi di emergenze locali o nazionali, informazioni UE classificate possano finire in mani di soggetti non autorizzati;

f) sovrintendere e coordinare, in tutti i settori di competenza, l'attuazione delle disposizioni per la sicurezza e la tutela delle informazioni UE classificate.

UFFICIO CENTRALE PER LA SICUREZZA.

5. Su disposizione dell'ANS:

   a) coordina l'attività degli organi centrali di sicurezza e controlla l'esatta applicazione delle norme che presiedono alla sicurezza e alla tutela delle informazioni UE classificate;

   b) assicura la registrazione, presso l'*ufficio centrale di registrazione* istituito nel suo ambito, dei documenti e materiali classificati UE-SEGRETISSIMO inviati all'Italia dall'Unione europea o dagli Stati membri, e viceversa, secondo le disposizioni contenute nella *Decisione del Consiglio dell'Ue del 19 marzo 2001* e le altre disposizioni di dettaglio emanate dall'ANS;

   c) tiene aggiornata la situazione dei documenti UE-SEGRETISSIMO ricevuti dall'Unione europea o Stati membri e da esso inoltrati agli organi centrali di sicurezza nazionali, nonché di quelli pervenuti agli stessi organi centrali di sicurezza ed, eventualmente, agli altri organi di sicurezza nazionali, direttamente dall'Unione europea o dagli Stati membri;

   d) esercita le attribuzioni di competenza in materia di abilitazioni di sicurezza UE;

   e) controlla e verifica, a livello centrale e periferico, mediante attività ispettiva diretta e delegata, ordinaria e straordinaria, l'attuazione delle disposizioni in materia di protezione e tutela delle informazioni, dei documenti e dei materiali UE classificati;

   f) partecipa, presso le istituzioni comunitarie ed enti nazionali, all'elaborazione di progetti normativi aventi ad oggetto la protezione e la tutela delle informazioni UE classificate;

   g) è organo nazionale di coordinamento e collegamento - ai fini della protezione e della tutela delle informazioni UE classificate - con:

      i) le istituzioni comunitarie;

      ii) le Autorità nazionali per la sicurezza dei Paesi membri dell'Unione europea;

      iii) organismi decentrati dell'Unione europea.

ORGANI CENTRALI DI SICUREZZA.

6. Sono organi centrali di sicurezza quelli a cui la legge, il regolamento o altre disposizioni amministrative attribuiscono, in ciascun ministero, forza armata, ente autonomo, associazione od organismo, la responsabilità di vertice in ordine alla direzione, coordinamento e controllo in materia di sicurezza e tutela delle informazioni classificate, sotto qualunque forma espresse e gestite. In particolare, gli organi centrali di sicurezza:

   a) coordinano e controllano, presso tutti gli organi di sicurezza tecnicamente dipendenti, sia a livello centrale sia a quello periferico, l'esatta applicazione di tutte le disposizioni inerenti alla protezione e alla tutela delle informazioni UE classificate;

   b) tengono aggiornato l'elenco del personale del proprio ente abilitato all'accesso alle informazioni classificate UE RISERVATISSIMO e superiore, custodendone, nei termini previsti, i relativi certificati;

   c) assolvono, nei limiti previsti dalle vigenti disposizioni, le attribuzioni in materia di rilascio, rinnovo, diniego, sospensione, declassifica, dequalifica e revoca dei nulla osta di sicurezza (NOS) per l'accesso alle informazioni classificate UE-RISERVATISSIMO e superiore;

   d) inoltrano all'ANS-UCSI proposte intese ad istituire, modificare o estinguere, nell'ambito dell'amministrazione centrale e periferica del proprio ente, organi di sicurezza UE.

ORGANI DI SICUREZZA.

7. Gli organi di sicurezza sono unità amministrative istituite per la gestione delle informazioni UE classificate, in via esclusiva o in concorso con altre categorie di informazioni classificate (nazionali, della NATO, dell'UEO, di altre organizzazioni internazionali e relativi ad altri accordi di sicurezza, bilaterali o multilaterali, stipulati dall'Italia con altri Paesi). In quest'ultimo caso ai già costituiti organi di sicurezza può essere rilasciata, quando necessaria, autorizzazione per la gestione anche delle informazioni UE classificate.

a) Gli organi di sicurezza istituiti esclusivamente per la gestione delle informazioni UE classificate si distinguono in:

   i) Segreterie Speciali UE/SS;

   ii) Segreterie UE/S;

   iii) Punti di Controllo UE/SS;Punti di Controllo UE/S.

b) Quando i seguenti organi di sicurezza:

   i) Segreterie Speciali COSMIC-FOCAL;

   ii) Segreterie NATO-UEO;

   iii) Punti di Controllo COSMIC-FOCAL;

   iv) Punti di Controllo NATO-UEO,

   già istituiti per la gestione di altre categorie di informazioni classificate (nazionali, della NATO, dell'UEO, di altre organizzazioni internazionali e relativi ad altri accordi di sicurezza, bilaterali o multilaterali, stipulati dall'Italia con altri Paesi) vengono autorizzati dall'ANS a gestire anche informazioni UE classificate, la loro denominazione è aggiornata come segue:

   v) Segreterie Speciali COSMIC-FOCAL-UE/SS;

   vi) Segreterie NATO-UEO-UE/S;

   vii) Punti di Controllo COSMIC-FOCAL-UE/SS;

   viii) Punti di Controllo NATO-UEO-UE/S.

c) Tutti gli organi di sicurezza autorizzati, in via esclusiva o non, alla gestione di informazioni UE classificate, assumono anche la denominazione di *organi di sicurezza UE*.

SEGRETERIE SPECIALI UE/SS O COSMIC-FOCAL-UE/SS.

8. Le Segreterie Speciali UE/SS o COSMIC-FOCAL-UE/SS sono organi di sicurezza istituiti nell'ambito degli organi centrali di sicurezza e di taluni enti centrali e periferici per la gestione anche dei documenti UE classificati fino alla massima classifica di segretezza UE-SEGRETISSIMO. Le suddette Segreterie Speciali, ai soli fini della tutela delle informazioni classificate UE-SEGRETISSIMO, sono anche denominate "*sottosezioni dell'ufficio centrale di registrazione UE-SEGRETISSIMO*" istituito presso l'ANS-UCSI.
Le Segreterie Speciali UE/SS o COSMIC-FOCAL-UE/SS, ai fini della tutela delle informazioni UE classificate, hanno il compito di:

   a) promuovere, nell'ambito del proprio ente, la conoscenza delle norme legislative e delle disposizioni amministrative concernenti la tutela delle informazioni UE classificate;

   b) istruire il personale del proprio ente sulle responsabilità connesse alla conoscenza e gestione delle informazioni UE classificate. Tale compito deve essere assolto con frequenza almeno annuale dal funzionario o ufficiale alla sicurezza dell'ente o, per sua delega, dal funzionario o ufficiale di controllo della Segreteria Speciale UE;

   c) tenere aggiornata la lista di accesso delle persone del proprio ente autorizzate all'accesso alle informazioni classificate UE-SEGRETISSIMO, secondo le designazioni stabilite dal Capo dell'ente o comando o, per sua delega, dal funzionario o ufficiale alla sicurezza, sulla base del principio della "*necessità di conoscere*";

   d) controllare e gestire i documenti UE classificati originati e ricevuti;tenere aggiornata la situazione di tutti i documenti classificati di cui sono responsabili, con particolare riguardo a quelli classificati UE-SEGRETISSIMO e UE-SEGRETO;

   e) tenere aggiornato il registro dei NOS del personale del proprio ente;

f) attuare le disposizioni di competenza relative alle richieste, per il personale del proprio ente o comando, per il rilascio e il rinnovo dei NOS per l'accesso alle informazioni classificate UE-RISERVATISSIMO o di grado superiore;

g) proporre al proprio organo centrale di sicurezza il ritiro dei NOS relativi al personale del proprio ente o comando che non ha più necessità di accedere alle informazioni classificate UE-RISERVATISSIMO o di grado superiore;

h) segnalare al proprio organo centrale di sicurezza ogni controindicazione, sotto il profilo dell'affidabilità ai fini della salvaguardia delle informazioni UE classificate, che si rilevi a carico del personale del proprio ente o comando per il quale sia stato rilasciato il NOS UE;

i) effettuare le ispezioni di sicurezza agli organi di sicurezza UE tecnicamente dipendenti;

l) segnalare all'ANS-UCSI i nominativi delle persone del proprio ente o comando designate ad attribuire alle informazioni, documenti e materiali, le classifiche di segretezza UE-SEGRETISSIMO e UE-SEGRETO;

m) ricevere, registrare, custodire e, ove previsto, inoltrare ai Punti di Controllo UE/SS tecnicamente dipendenti i documenti UE-SEGRETISSIMO ricevuti dall'ufficio centrale di registrazione UE-SEGRETISSIMO dell'ANS-UCSI o direttamente da altri enti nazionali, dall'Unione europea o dai Paesi membri;

n) segnalare all'ANS-UCSI gli estremi dei documenti UE-SEGRETISSIMO ricevuti non per il suo tramite;

o) inoltrare all'ANS-UCSI, per il tramite del proprio organo centrale di sicurezza, proposte intese ad istituire o ad abolire, nell'ambito del proprio ente o comando, organi di sicurezza UE;

p) comunicare all'ANS-UCSI e al proprio organo centrale di sicurezza, i nominativi dei funzionari o ufficiali di controllo, e relativi sostituti, degli organi di sicurezza UE tecnicamente dipendenti;

q) segnalare con tempestività all'ANS-UCSI, o all'organo centrale di sicurezza interessato o all'organismo comunitario o internazionale competente il livello del NOS UE relativo al personale del proprio ente o comando designato a partecipare a conferenze o riunioni UE classificate;

r) effettuare annualmente l'inventario e il controllo dei documenti classificati UE-SEGRETISSIMO in carico e trasmettere all'ANS-UCSI, ufficio centrale di registrazione UE-SEGRETISSIMO, i verbali di distruzione relativi a tali documenti, unitamente al registro d'inventario, per la parifica.

SEGRETERIE UE/S O NATO-UEO-UE/S

9. Le Segreterie UE/S o NATO-UEO-UE/S sono organi di sicurezza istituiti per la gestione dei documenti UE classificati fino al livello UE-SEGRETO.
Le SegreterieUE/S o NATO-UEO-UE/S hanno il compito di:

a) promuovere, nell'ambito del proprio ente o comando, la conoscenza delle norme legislative e delle disposizioni amministrative concernenti la tutela delle informazioni UE classificate;

b) istruire il personale del proprio ente, per il quale è stato rilasciato il NOS UE, sulle responsabilità connesse alla conoscenza e gestione delle informazioni UE classificate. Tale compito è assolto, con frequenza almeno annuale, dal funzionario o ufficiale alla sicurezza dell'ente o, per sua delega, dal funzionario o ufficiale di controllo della Segreteria UE/S;

c) tenere aggiornata la lista di accesso delle persone del proprio ente autorizzate all'accesso alle informazioni UE-SEGRETO secondo le designazioni stabilite dal Capo dell'ente o, per sua delega, dal funzionario o ufficiale alla sicurezza sulla base del principio della "necessità di conoscere";

d) controllare e gestire i documenti UE classificati originati e ricevuti;

e) tenere aggiornata la situazione dei documenti UE classificati di cui sono responsabili, con particolare riguardo a quelli classificati UE-SEGRETO;

f) tenere aggiornato il registro dei NOS UE del personale del proprio ente o comando;

g) attuare le disposizioni di competenza relative alle richieste per il rilascio e il rinnovo dei NOS UE per il personale del proprio ente o comando;

h) proporre al proprio organo centrale di sicurezza il ritiro dei NOS UE relativi al personale del proprio ente o comando che non ha più necessità di accedere alle informazioni UE classificate;

i) segnalare al proprio organo centrale di sicurezza ogni controindicazione, sotto il profilo dell'affidabilità ai fini della salvaguardia delle informazioni UE classificate, che si rilevi a carico del personale del proprio ente o comando per il quale sia stato rilasciato il NOS UE;

l) effettuare, mediante il funzionario o ufficiale alla sicurezza o, per sua delega, il funzionario o ufficiale di controllo, le ispezioni di sicurezza agli organi di sicurezza UE tecnicamente dipendenti;

m) ricevere, registrare, custodire e, ove previsto, inoltrare ad altri Punti di Controllo UE/S tecnicamente dipendenti i documenti UE classificati ricevuti;

n) inoltrare all'ANS-UCSI, per il tramite del proprio organo centrale di sicurezza, proposte intese ad istituire o ad abolire, nell'ambito del proprio ente o comando, dipendenti Punti di Controllo UE/S;

o) comunicare all'ANS-UCSI e al proprio organo centrale di sicurezza, i nominativi dei funzionari o ufficiali di controllo, e relativi sostituti, dei Punti di Controllo UE/S tecnicamente dipendenti;

p) segnalare con tempestività all'ANS-UCSI o all'organo centrale di sicurezza interessato o all'organismo comunitario o internazionale competente, il livello del NOS UE del personale del proprio ente designato a partecipare a conferenze o riunioni UE classificate, in Italia o all'estero.

PUNTI DI CONTROLLO UE/SS O COSMIC-FOCAL-UE/SS

10. I Punti di Controllo UE/SS o COSMIC-FOCAL-UE/SS sono organi di sicurezza istituiti nell'ambito degli enti e comandi, centrali e periferici, per la gestione dei documenti UE classificati fino al livello UE-SEGRETISSIMO. Essi dipendono, in linea tecnica, dalla Segreteria Speciale UE/SS o COSMIC-FOCAL-UE/SS istituita nell'ambito dell'organo centrale di sicurezza. I suddetti Punti di Controllo, ai soli fini della tutela delle informazioni classificate UE-SEGRETISSIMO, sono anche altrimenti detti "sottosezioni dell'ufficio centrale di registrazione UE-SEGRETISSIMO" istituito presso l'ANS-UCSI.
I Punti di Controllo UE/SS o COSMIC-FOCAL-UE/SS hanno il compito di:

a) promuovere, nell'ambito del proprio ente, la conoscenza delle norme legislative e delle disposizioni amministrative concernenti la tutela delle informazioni UE classificate;

b) istruire il personale del proprio ente, per il quale è stato rilasciato il NOS UE, sulle responsabilità connesse alla conoscenza e gestione delle informazioni UE classificate. Tale compito è assolto, con frequenza almeno annuale, dal funzionario o ufficiale alla sicurezza dell'ente o, per sua delega, dal funzionario o ufficiale di controllo dell'organo di sicurezza;

c) tenere aggiornata la lista di accesso relativa alle persone del proprio ente autorizzate a conoscere informazioni classificate UE-SEGRETISSIMO e UE-SEGRETO, secondo le designazioni stabilite dal Capo dell'ente o, per sua delega, dal funzionario o ufficiale alla sicurezza, sulla base del principio della "necessità di conoscere";

d) controllare e gestire i documenti UE classificati originati e ricevuti;

e) tenere aggiornata la situazione di tutti i documenti classificati di cui sono responsabili, con particolare riguardo a quelli classificati UE-SEGRETISSIMO e UE-SEGRETO;

f) effettuare annualmente l'inventario e il controllo dei documenti UE-SEGRETISSIMO" in carico, e trasmettere all'ANS-UCSI i verbali di distruzione relativi a tali documenti, unitamente al registro d'inventario, per la parifica;

g) tenere aggiornato il registro dei NOS UE del personale del proprio ente;

h) attuare le disposizioni di competenza relative alle richieste per il rilascio e il rinnovo dei NOS UE per il personale del proprio ente;

i) proporre al proprio organo centrale di sicurezza il ritiro dei NOS UE relativi al personale del proprio ente che non ha più necessità di accedere alle informazioni UE classificate;

l) segnalare alla Segreteria Speciale UE da cui dipendono in linea tecnica ogni controindicazione, sotto il profilo dell'affidabilità ai fini della salvaguardia delle informazioni UE classificate, che si rilevi a carico del personale del proprio ente per il quale sia stato rilasciato il NOS UE;

m) effettuare le ispezioni agli organi di sicurezza UE tecnicamente dipendenti;

n) segnalare all'ANS-UCSI i nominativi delle persone del proprio ente designate ad attribuire alle informazioni, documenti e materiali la classifica UE-SEGRETISSIMO;

o) registrare e custodire i documenti UE-SEGRETISSIMO ricevuti per il tramite dell'ANS-UCSI o direttamente da altri enti nazionali, dall'Unione europea o dagli Stati membri;

p) segnalare all'ANS-UCSI gli estremi dei documenti UE-SEGRETISSIMO ricevuti non per il suo tramite;

q) segnalare con tempestività all'organo di sicurezza nazionale interessato o all'organismo comunitario o internazionale competente il livello del NOS UE relativo al personale del proprio ente designato a partecipare, in Italia o all'estero, a conferenze o riunioni UE classificate;

r) effettuare annualmente l'inventario e il controllo di tutti i documenti UE-SEGRETISSIMO in carico e trasmettere all'ANS-UCSI tutti i verbali di distruzione relativi a tali documenti, unitamente al registro d'inventario, per la parifica.

I Punti di Controllo UE/SS, salvo che non venga diversamente disposto dalla Segreteria Speciale UE da cui dipendono in linea tecnica, possono ricevere e spedire i documenti UE-SEGRETISSIMO solo per il tramite di quest'ultima. Tutti gli altri documenti UE classificati possono essere ricevuti e spediti anche senza il tramite della predetta Segreteria Speciale UE.

I Punti di Controllo UE/SS possono, in caso di emergenza o quando lo esigono particolari motivi, inviare ad altri Punti di Controllo UE/SS o Segreterie Speciali UE/SS di altri enti, senza il tramite della Segreteria Speciale UE da cui essi dipendono in linea tecnica, i documenti UE-SEGRETISSIMO.

PUNTI DI CONTROLLO UE/S O NATO-UEO-UE/S.

11. I Punti di Controllo UE/S o NATO-UEO-UE/S sono organi di sicurezza istituiti nell'ambito degli enti e comandi, centrali e periferici, per la gestione dei documenti UE classificati fino al livello UE-SEGRETO. Essi dipendono, in linea tecnica, dalla Segreteria Speciale UE/SS (o COSMIC-FOCAL-UE/SS), o dal Punto di Controllo UE/SS (o COSMIC-FOCAL-UE/SS), o dalla Segreteria UE-S (o NATO-UEO-UE/S), sovraordinati.
I Punti di Controllo UE/S o NATO-UEO-UE/S hanno il compito di:

a) promuovere, nell'ambito del proprio ente o comando, la conoscenza delle norme legislative e delle disposizioni amministrative concernenti la tutela delle informazioni UE classificate;

b) istruire il personale del proprio ente o comando, per il quale è stato rilasciato il NOS UE, sulle responsabilità connesse alla conoscenza e gestione delle informazioni UE classificate. Tale compito è assolto, con frequenza almeno annuale, dal funzionario o ufficiale alla sicurezza dell'ente o, per sua delega, dal funzionario o ufficiale di controllo dell'organo di sicurezza;

c) tenere aggiornata la lista di accesso relativa alle persone del proprio ente o comando autorizzate a conoscere informazioni nazionali classificate UE-SEGRETO" secondo le designazioni stabilite dal Capo dell'ente o dal funzionario o ufficiale alla sicurezza, o dal responsabile dell'unità amministrativa direttamente interessato, sulla base del principio della "*necessità di conoscere*";

d) controllare e gestire i documenti UE classificati originati e ricevuti;

e) tenere aggiornata la situazione di tutti i documenti UE classificati di cui sono responsabili, con particolare riguardo a quelli classificati UE-SEGRETO;

f) effettuare annualmente l'inventario e il controllo interni di tutti i documenti UE classificati di cui si ha la responsabilità;

g) tenere aggiornato il registro dei NOS UE relativi al personale del proprio ente o comando;

h) attuare le disposizioni di competenza relative alle richieste per il rilascio e il rinnovo dei NOS UE del personale del proprio ente;

i) proporre al proprio organo centrale di sicurezza il ritiro dei NOS UE relativi al personale del proprio ente o comando che non ha più necessità di accedere alle informazioni UE classificate;

l) segnalare al proprio organo centrale di sicurezza ogni controindicazione, sotto il profilo dell'affidabilità ai fini della salvaguardia delle informazioni UE classificate, che si rilevi a carico del personale del proprio ente o comando per il quale sia stato rilasciato il NOS UE;

m) segnalare con tempestività all'organo di sicurezza nazionale interessato o all'organismo comunitario o internazionale competente il livello del NOS UE relativo al personale del proprio ente o comando designato a partecipare, in Italia o all'estero, a conferenze o riunioni UE classificate.

02A07317

GIANFRANCO TATOZZI, *direttore* FRANCESCO NOCITA, *redattore*

(5651427/1) Roma, 2002 - Istituto Poligrafico e Zecca dello Stato - S.

ISTITUTO POLIGRAFICO E ZECCA DELLO STATO

LIBRERIE CONCESSIONARIE PRESSO LE QUALI È IN VENDITA LA GAZZETTA UFFICIALE

ABRUZZO

◇ **CHIETI**
LIBRERIA PIROLA MAGGIOLI - DE LUCA
Via A. Herio, 21

◇ **PESCARA**
LIBRERIA COSTANTINI DIDATTICA
Corso V. Emanuele, 146
LIBRERIA DELL'UNIVERSITÀ
Via Galilei (ang. via Gramsci)

◇ **SULMONA**
LIBRERIA UFFICIO IN
Circonv. Occidentale, 10

◇ **TERAMO**
LIBRERIA DE LUCA
Via Riccitelli, 6

BASILICATA

◇ **MATERA**
LIBRERIA MONTEMURRO
Via delle Beccherie, 69
GULLIVER LIBRERIE
Via del Corso, 32

◇ **POTENZA**
LIBRERIA PAGGI ROSA
Via Pretoria

CALABRIA

◇ **CATANZARO**
LIBRERIA NISTICÒ
Via A. Daniele, 27

◇ **COSENZA**
LIBRERIA DOMUS
Via Monte Santo, 70/A

◇ **PALMI**
LIBRERIA IL TEMPERINO
Via Roma, 31

◇ **REGGIO CALABRIA**
LIBRERIA L'UFFICIO
Via B. Buozzi, 23/A/B/C

◇ **VIBO VALENTIA**
LIBRERIA AZZURRA
Corso V. Emanuele III

CAMPANIA

◇ **ANGRI**
CARTOLIBRERIA AMATO
Via dei Goti, 11

◇ **AVELLINO**
LIBRERIA GUIDA 3
Via Vasto, 15
LIBRERIA PIROLA MAGGIOLI
Via Matteotti, 30-32
CARTOLIBRERIA CESA
Via G. Nappi, 47

◇ **BENEVENTO**
LIBRERIA LA GIUDIZIARIA
Via F. Paga, 11
LIBRERIA MASONE
Viale Rettori, 71

◇ **CASERTA**
LIBRERIA GUIDA 3
Via Caduti sul Lavoro, 29-33

◇ **CASTELLAMMARE DI STABIA**
LINEA SCUOLA
Via Raiola, 69/D

◇ **CAVA DEI TIRRENI**
LIBRERIA RONDINELLA
Corso Umberto I, 253

◇ **ISCHIA PORTO**
LIBRERIA GUIDA 3
Via Sogliuzzo

◇ **NAPOLI**
LIBRERIA LEGISLATIVA MAJOLO
Via Caravita, 30
LIBRERIA GUIDA 1
Via Portalba, 20-23
LIBRERIA GUIDA 2
Via Merliani, 118
LIBRERIA I.B.S.
Salita del Casale, 18

◇ **NOCERA INFERIORE**
LIBRERIA LEGISLATIVA CRISCUOLO
Via Fava, 51;

◇ **NOLA**
LIBRERIA EDITRICE LA RICERCA
Via Fonseca, 59

◇ **POLLA**
CARTOLIBRERIA GM
Via Crispi

◇ **SALERNO**
LIBRERIA GUIDA
Corso Garibaldi, 142

EMILIA-ROMAGNA

◇ **BOLOGNA**
LIBRERIA GIURIDICA CERUTI
Piazza Tribunali, 5/F
LIBRERIA PIROLA MAGGIOLI
Via Castiglione, 1/C
GIURIDICA EDINFORM
Via delle Scuole, 38

◇ **CARPI**
LIBRERIA BULGARELLI
Corso S. Cabassi, 15

◇ **CESENA**
LIBRERIA BETTINI
Via Vescovado, 5

◇ **FERRARA**
LIBRERIA PASELLO
Via Canonica, 16-18

◇ **FORLÌ**
LIBRERIA CAPPELLI
Via Lazzaretto, 51
LIBRERIA MODERNA
Corso A. Diaz, 12

◇ **MODENA**
LIBRERIA GOLIARDICA
Via Berengario, 60

◇ **PARMA**
LIBRERIA PIROLA PARMA
Via Farini, 34/D

◇ **RAVENNA**
LIBRERIA GIURIDICA DI FERMANI MAURIZIO
Via Corrado Ricci, 12

◇ **REGGIO EMILIA**
LIBRERIA MODERNA
Via Farini, 1/M

◇ **RIMINI**
LIBRERIA DEL PROFESSIONISTA
Via XXII Giugno, 3

FRIULI-VENEZIA GIULIA

◇ **GORIZIA**
CARTOLIBRERIA ANTONINI
Via Mazzini, 16

◇ **PORDENONE**
LIBRERIA MINERVA
Piazzale XX Settembre, 22/A

◇ **TRIESTE**
LIBRERIA TERGESTE
Piazza Borsa, 15 (gall. Tergesteo)

◇ **UDINE**
LIBRERIA BENEDETTI
Via Mercatovecchio, 13
LIBRERIA TARANTOLA
Via Vittorio Veneto, 20

LAZIO

◇ **FROSINONE**
LIBRERIA EDICOLA CARINCI
Piazza Madonna della Neve, s.n.c.

◇ **LATINA**
LIBRERIA GIURIDICA LA FORENSE
Viale dello Statuto, 28-30

◇ **RIETI**
LIBRERIA LA CENTRALE
Piazza V. Emanuele, 8

◇ **ROMA**
LIBRERIA ECONOMICO GIURIDICA
Via S. Maria Maggiore, 121
LIBRERIA DE MIRANDA
Viale G. Cesare, 51/E-F-G
LIBRERIA LAURUS ROBUFFO
Via San Martino della Battaglia, 35
LIBRERIA L'UNIVERSITARIA
Viale Ippocrate, 99
LIBRERIA IL TRITONE
Via Tritone, 61/A
LIBRERIA MEDICHINI
Via Marcantonio Colonna, 68-70
LA CONTABILE
Via Tuscolana, 1027

◇ **SORA**
LIBRERIA PIROLA MAGGIOLI
Via Abruzzo, 4

◇ **TIVOLI**
LIBRERIA MANNELLI
Viale Mannelli, 10

◇ **VITERBO**
LIBRERIA "AR"
Palazzo Uffici Finanziari - Loc. Pietrare
LIBRERIA DE SANTIS
Via Venezia Giulia, 5

LIGURIA

◇ **CHIAVARI**
CARTOLERIA GIORGINI
Piazza N.S. dell'Orto, 37-38

◇ **GENOVA**
LIBRERIA GIURIDICA DI A. TERENGHI & DARIO CERIOLI
Galleria E. Martino, 9

◇ **IMPERIA**
LIBRERIA PIROLA MAGGIOLI - DI VIALE
Viale Matteotti, 43/A-45

LOMBARDIA

◇ **BRESCIA**
LIBRERIA QUERINIANA
Via Trieste, 13

◇ **BRESSO**
LIBRERIA CORRIDONI
Via Corridoni, 11

◇ **BUSTO ARSIZIO**
CARTOLIBRERIA CENTRALE BORAGNO
Via Milano, 4

◇ **COMO**
LIBRERIA GIURIDICA BERNASCONI
Via Mentana, 15

◇ **GALLARATE**
LIBRERIA PIROLA MAGGIOLI
Via Pulicelli, 1 (ang. p. risorgimento)
LIBRERIA TOP OFFICE
Via Torino, 8

◇ **LECCO**
LIBRERIA PIROLA - DI LAZZARINI
Corso Mart. Liberazione, 100/A

◇ **LODI**
LA LIBRERIA S.a.s.
Via Defendente, 32

◇ **MANTOVA**
LIBRERIA ADAMO DI PELLEGRINI
Corso Umberto I, 32

◇ **MILANO**
LIBRERIA CONCESSIONARIA
IPZS-CALABRESE
Galleria V. Emanuele II, 13-15
FOROBONAPARTE S.r.l.
Foro Bonaparte, 53

◇ **MONZA**
LIBRERIA DELL'ARENGARIO
Via Mapelli, 4

◇ **PAVIA**
LIBRERIA GALASSIA
Corso Mazzini, 28

◇ **VARESE**
LIBRERIA PIROLA - DI MITRANO
Via Albuzzi, 8

Segue: **LIBRERIE CONCESSIONARIE PRESSO LE QUALI È IN VENDITA LA GAZZETTA UFFICIALE**

MARCHE

◇ **ANCONA**
LIBRERIA FOGOLA
Piazza Cavour, 4-5-6
◇ **ASCOLI PICENO**
LIBRERIA PROSPERI
Largo Crivelli, 8
◇ **MACERATA**
LIBRERIA UNIVERSITARIA
Via Don Minzoni, 6
◇ **PESARO**
LIBRERIA PROFESSIONALE MARCHIGIANA
Via Mameli, 34
◇ **S. BENEDETTO DEL TRONTO**
LA BIBLIOFILA
Via Ugo Bassi, 38

MOLISE

◇ **CAMPOBASSO**
LIBRERIA GIURIDICA DI.E.M.
Via Capriglione, 42-44
CENTRO LIBRARIO MOLISANO
Viale Manzoni, 81-83

PIEMONTE

◇ **ALBA**
CASA EDITRICE I.C.A.P.
Via Vittorio Emanuele, 19
◇ **ALESSANDRIA**
LIBRERIA INTERNAZIONALE BERTOLOTTI
Corso Roma, 122
◇ **BIELLA**
LIBRERIA GIOVANNACCI
Via Italia, 14
◇ **CUNEO**
CASA EDITRICE ICAP
Piazza dei Galimberti, 10
◇ **NOVARA**
EDIZIONI PIROLA E MODULISTICA
Via Costa, 32
◇ **TORINO**
LIBRERIA DEGLI UFFICI
Corso Vinzaglio, 11
◇ **VERBANIA**
LIBRERIA MARGAROLI
Corso Mameli, 55 - Intra
◇ **VERCELLI**
CARTOLIBRERIA COPPO
Via Galileo Ferraris, 70

PUGLIA

◇ **ALTAMURA**
LIBRERIA JOLLY CART
Corso V. Emanuele, 16
◇ **BARI**
CARTOLIBRERIA QUINTILIANO
Via Arcidiacono Giovanni, 9
LIBRERIA PALOMAR
Via P. Amedeo, 176/B
LIBRERIA LATERZA GIUSEPPE & FIGLI
Via Sparano, 134
LIBRERIA FRATELLI LATERZA
Via Crisanzio, 16
◇ **BRINDISI**
LIBRERIA PIAZZO
Corso Garibaldi, 38/A
◇ **CERIGNOLA**
LIBRERIA VASCIAVEO
Via Gubbio, 14
◇ **FOGGIA**
LIBRERIA PATIERNO
Via Dante, 21
◇ **LECCE**
LIBRERIA LECCE SPAZIO VIVO
Via Palmieri, 30
◇ **MANFREDONIA**
LIBRERIA IL PAPIRO
Corso Manfredi, 126
◇ **MOLFETTA**
LIBRERIA IL GHIGNO
Via Campanella, 24
◇ **TARANTO**
LIBRERIA FUMAROLA
Corso Italia, 229

SARDEGNA

◇ **CAGLIARI**
LIBRERIA F.LLI DESSÌ
Corso V. Emanuele, 30-32
◇ **ORISTANO**
LIBRERIA CANU
Corso Umberto I, 19
◇ **SASSARI**
LIBRERIA MESSAGGERIE SARDE
Piazza Castello, 11
LIBRERIA AKA
Via Roma, 42

SICILIA

◇ **ACIREALE**
LIBRERIA S.G.C. ESSEGICI S.a.s.
Via Caronda, 8-10
CARTOLIBRERIA BONANNO
Via Vittorio Emanuele, 194
◇ **AGRIGENTO**
TUTTO SHOPPING
Via Panoramica dei Templi, 17
◇ **CALTANISSETTA**
LIBRERIA SCIASCIA
Corso Umberto I, 111
◇ **CASTELVETRANO**
CARTOLIBRERIA MAROTTA & CALIA
Via Q. Sella, 106-108
◇ **CATANIA**
LIBRERIA LA PAGLIA
Via Etnea, 393
LIBRERIA ESSEGICI
Via F. Riso, 56
LIBRERIA RIOLO FRANCESCA
Via Vittorio Emanuele, 137
◇ **GIARRE**
LIBRERIA LA SENORITA
Corso Italia, 132-134
◇ **MESSINA**
LIBRERIA PIROLA MESSINA
Corso Cavour, 55
◇ **PALERMO**
LIBRERIA S.F. FLACCOVIO
Via Ruggero Settimo, 37
LIBRERIA FORENSE
Via Maqueda, 185
LIBRERIA S.F. FLACCOVIO
Piazza V. E. Orlando, 15-19
LIBRERIA MERCURIO LI.CA.M.
Piazza S. G. Bosco, 3
LIBRERIA DARIO FLACCOVIO
Viale Ausonia, 70
LIBRERIA CICALA INGUAGGIATO
Via Villaermosa, 28
LIBRERIA SCHOOL SERVICE
Via Galletti, 225
◇ **S. GIOVANNI LA PUNTA**
LIBRERIA DI LORENZO
Via Roma, 259
◇ **SIRACUSA**
LA LIBRERIA DI VALVO E SPADA
Piazza Euripide, 22
◇ **TRAPANI**
LIBRERIA LO BUE
Via Cascio Cortese, 8

TOSCANA

◇ **AREZZO**
LIBRERIA PELLEGRINI
Via Cavour, 42
◇ **FIRENZE**
LIBRERIA PIROLA «già Etruria»
Via Cavour, 46/R
LIBRERIA MARZOCCO
Via de' Martelli, 22/R
LIBRERIA ALFANI
Via Alfani, 84-86/R
◇ **GROSSETO**
NUOVA LIBRERIA
Via Mille, 6/A
◇ **LIVORNO**
LIBRERIA AMEDEO NUOVA
Corso Amedeo, 23-27
LIBRERIA IL PENTAFOGLIO
Via Fiorenza, 4/B
◇ **LUCCA**
LIBRERIA BARONI ADRI
Via S. Paolino, 45-47
LIBRERIA SESTANTE
Via Montanara, 37
◇ **MASSA**
LIBRERIA IL MAGGIOLINO
Via Europa, 19
◇ **PISA**
LIBRERIA VALLERINI
Via dei Mille, 13
◇ **PISTOIA**
LIBRERIA UNIVERSITARIA TURELLI
Via Macallè, 37
◇ **PRATO**
LIBRERIA GORI
Via Ricasoli, 25
◇ **SIENA**
LIBRERIA TICCI
Via delle Terme, 5-7
◇ **VIAREGGIO**
LIBRERIA IL MAGGIOLINO
Via Puccini, 38

TRENTINO-ALTO ADIGE

◇ **TRENTO**
LIBRERIA DISERTORI
Via Diaz, 11

UMBRIA

◇ **FOLIGNO**
LIBRERIA LUNA
Via Gramsci, 41
◇ **PERUGIA**
LIBRERIA SIMONELLI
Corso Vannucci, 82
LIBRERIA LA FONTANA
Via Sicilia, 53
◇ **TERNI**
LIBRERIA ALTEROCCA
Corso Tacito, 29

VENETO

◇ **BELLUNO**
LIBRERIA CAMPDEL
Piazza Martiri, 27/D
◇ **CONEGLIANO**
LIBRERIA CANOVA
Via Cavour, 6/B
◇ **PADOVA**
LIBRERIA DIEGO VALERI
Via Roma, 114
◇ **ROVIGO**
CARTOLIBRERIA PAVANELLO
Piazza V. Emanuele, 2
◇ **TREVISO**
CARTOLIBRERIA CANOVA
Via Calmaggiore, 31
◇ **VENEZIA-MESTRE**
LIBRERIA SAMBO
Via Torre Belfredo, 60
◇ **VERONA**
LIBRERIA L.E.G.I.S.
Via Adigetto, 43
LIBRERIA GIURIDICA EDITRICE
Via Costa, 5
◇ **VICENZA**
LIBRERIA GALLA 1880
Corso Palladio, 11

MODALITÀ PER LA VENDITA

La «Gazzetta Ufficiale» e tutte le altre pubblicazioni ufficiali sono in vendita al pubblico:
— presso l'Agenzia dell'Istituto Poligrafico e Zecca dello Stato in ROMA: piazza G. Verdi, 10 - ☎ 06 85082147;
— presso le Librerie concessionarie indicate nelle pagine precedenti.

Le richieste per corrispondenza devono essere inviate all'Istituto Poligrafico e Zecca dello Stato - Gestione Gazzetta Ufficiale - Piazza G. Verdi, 10 - 00100 Roma, versando l'importo, maggiorato delle spese di spedizione, a mezzo del c/c postale **n. 16716029.** Le inserzioni, come da norme riportate nella testata della parte seconda, si ricevono con pagamento anticipato, presso le agenzie in Roma e presso le librerie concessionarie.

PREZZI E CONDIZIONI DI ABBONAMENTO - 2002
(Salvo conguaglio)

Gli abbonamenti annuali hanno decorrenza dal 1° gennaio e termine al 31 dicembre 2002
i semestrali dal 1° gennaio al 30 giugno 2002 e dal 1° luglio al 31 dicembre 2002

PARTE PRIMA - SERIE GENERALE E SERIE SPECIALI
Gli abbonamenti tipo A, A1, F, F1 comprendono gli indici mensili

	Euro
Tipo A - Abbonamento ai fascicoli della serie generale, inclusi tutti i supplementi ordinari:	
- annuale	**271,00**
- semestrale	**154,00**
Tipo A1 - Abbonamento ai fascicoli della serie generale, inclusi i supplementi ordinari contenenti i provvedimenti legislativi:	
- annuale	**222,00**
- semestrale	**123,00**
Tipo A2 - Abbonamento ai supplementi ordinari contenenti i provvedimenti non legislativi:	
- annuale	**61,00**
- semestrale	**36,00**
Tipo B - Abbonamento ai fascicoli della serie speciale destinata agli atti dei giudizi davanti alla Corte costituzionale:	
- annuale	**57,00**
- semestrale	**37,00**
Tipo C - Abbonamento ai fascicoli della serie speciale destinata agli atti delle Comunità europee:	
- annuale	**145,00**
- semestrale	**80,00**
Tipo D - Abbonamento ai fascicoli della serie speciale destinata alle leggi ed ai regolamenti regionali:	
- annuale	**56,00**
- semestrale	**35,00**
Tipo E - Abbonamento ai fascicoli della serie speciale destinata ai concorsi indetti dallo Stato e dalle altre pubbliche amministrazioni:	
- annuale	**142,00**
- semestrale	**77,00**
Tipo F - *Completo.* Abbonamento ai fascicoli della serie generale, inclusi i supplementi ordinari contenenti i provvedimenti legislativi e non legislativi ed ai fascicoli delle quattro serie speciali (ex tipo F):	
- annuale	**586,00**
- semestrale	**316,00**
Tipo F1 - Abbonamento ai fascicoli della serie generale inclusi i supplementi ordinari contenenti i *provvedimenti legislativi ed ai fascicoli delle* quattro serie speciali (escluso il tipo A2):	
- annuale	**524,00**
- semestrale	**277,00**

Integrando con la somma di **€ 80,00** *il versamento relativo al tipo di abbonamento della* Gazzetta Ufficiale - *parte prima - prescelto, si riceverà anche l'Indice repertorio annuale cronologico per materie 2002.*

Prezzo di vendita di un fascicolo separato della *serie generale*	**0,77**
Prezzo di vendita di un fascicolo separato delle *serie speciali I, II e III*, ogni 16 pagine o frazione	**0,80**
Prezzo di vendita di un fascicolo della *IV serie speciale «Concorsi ed esami»*	**1,50**
Prezzo di vendita di un fascicolo *indici mensili*, ogni 16 pagine o frazione	**0,80**
Supplementi ordinari per la vendita a fascicoli separati, ogni 16 pagine o frazione	**0,80**
Supplementi straordinari per la vendita a fascicoli, ogni 16 pagine o frazione	**0,80**

Supplemento straordinario «Bollettino delle estrazioni»

Abbonamento annuale	**86,00**
Prezzo di vendita di un fascicolo, ogni 16 pagine o frazione	**0,80**

Supplemento straordinario «Conto riassuntivo del Tesoro»

Abbonamento annuale	**55,00**
Prezzo di vendita di un fascicolo separato	**5,00**

PARTE SECONDA - INSERZIONI

Abbonamento annuale	**253,00**
Abbonamento semestrale	**151,00**
Prezzo di vendita di un fascicolo, ogni 16 pagine o frazione	**0,85**

Raccolta Ufficiale degli Atti Normativi

Abbonamento annuo	**188,00**
Abbonamento annuo per Regioni, Province e Comuni	**175,00**
Volume separato	**17,50**

TARIFFE INSERZIONI
(densità di scrittura, fino a 77 caratteri/riga, nel conteggio si comprendono punteggiature e spazi)

Inserzioni Commerciali per ogni riga, o frazione di riga	**20,24**
Inserzioni Giudiziarie per ogni riga, o frazione di riga	**7,95**

I supplementi straordinari non sono compresi in abbonamento.
I prezzi di vendita, in abbonamento ed a fascicoli separati, per l'estero, *nonché quelli di vendita dei fascicoli delle* annate arretrate, *compresi i fascicoli dei supplementi ordinari e straordinari, sono* raddoppiati.

L'importo degli abbonamenti deve essere versato sul c/c postale n. 16716029 intestato all'Istituto Poligrafico e Zecca dello Stato. L'invio dei fascicoli disguidati, che devono essere richiesti entro 30 giorni dalla data di pubblicazione, è subordinato alla trasmissione dei dati riportati sulla relativa fascetta di abbonamento.

Per informazioni, prenotazioni o reclami attinenti agli abbonamenti oppure alla vendita della *Gazzetta Ufficiale* bisogna rivolgersi direttamente all'Amministrazione, presso l'Istituto Poligrafico e Zecca dello Stato - Piazza G. Verdi, 10 - 00100 ROMA

Gestione Gazzetta Ufficiale Abbonamenti Vendite	Ufficio inserzioni	Numero verde
☎ 800-864035 - Fax 06-85082520	☎ 800-864035 - Fax 06-85082242	☎ 800-864035